LTE6100

LTE Outdoor Gateway

User's Guide

Default Login Details

Web Address	http://192.168.1.1
Admin's User Name and Password	admin / 1234
Guest's User Name and Password	user / 1234

Edition 1, 7/2012

ZyXEL

www.zyxel.com

Copyright © 2012
ZyXEL Communications Corporation

IMPORTANT!

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the LTE Device and access the Web Configurator wizards. (See the wizard real time help for information on configuring each screen.) It also contains a connection diagram and package contents list.

Note: It is recommended you use the Web Configurator to configure the LTE Device.

Contents Overview

User's Guide 11

Introduction 13
Introducing the Web Configurator 17

Technical Reference 23

Connection Status and System Info 25
Broadband 31
Home Networking 39
Routing 45
Quality of Service (QoS) 49
Network Address Translation (NAT) 59
Dynamic DNS 67
Firewall 69
MAC Filter 79
Parental Control 81
VPN 85
Logs 99
Traffic Status 101
User Account 105
Remote MGMT 107
System 109
Time Setting 111
Log Setting 113
Firmware Upgrade 115
Backup/Restore 117
Diagnostic 121
Troubleshooting 123

Table of Contents

Contents Overview **3**

Table of Contents **5**

Part I: User's Guide **11**

Chapter 1
Introduction **13**

1.1 Overview 13
1.2 Applications for the LTE Device 13
1.2.1 Internet Access 13
1.3 Ways to Manage the LTE Device 14
1.4 Good Habits for Managing the LTE Device 14
1.5 LEDs (Lights) 14
1.6 The RESET Button 15

Chapter 2
Introducing the Web Configurator **17**

2.1 Overview 17
2.1.1 Accessing the Web Configurator 17
2.2 The Web Configurator Layout 19
2.2.1 Title Bar 19
2.2.2 Main Window 20
2.2.3 Traffic Status 20
2.2.4 User Account 20
2.2.5 Navigation Panel 21

Part II: Technical Reference **23**

Chapter 3
Connection Status and System Info **25**

3.1 Overview 25
3.2 The Connection Status Screen 25
3.3 The System Info Screen 27

Chapter 4
Broadband **31**

4.1 Overview 31
4.1.1 What You Can Do in this Chapter 31
4.1.2 What You Need to Know 31
4.1.3 Before You Begin 32
4.2 The Broadband Screen 32
4.2.1 Edit Internet Connection 32
4.3 The SIM Screen 33
4.3.1 PUK Code Screen 34
4.4 Technical Reference 35

Chapter 5
Home Networking 39

5.1 Overview 39
5.1.1 What You Can Do in this Chapter 39
5.1.2 What You Need To Know 39
5.2 The LAN Setup Screen 41
5.3 The Static DHCP Screen 42
5.3.1 Before You Begin 42
5.4 The UPnP Screen 43

Chapter 6
Routing 45

6.1 Overview 45
6.2 Configuring Static Route 46
6.2.1 Add/Edit Static Route 47

Chapter 7
Quality of Service (QoS) 49

7.1 Overview 49
7.1.1 What You Can Do in this Chapter 49
7.1.2 What You Need to Know 49
7.2 The QoS General Screen 50
7.3 The Queue Setup Screen 51
7.3.1 Add/Edit a QoS Queue 52
7.4 The Class Setup Screen 52
7.4.1 Add/Edit QoS Class 54
7.5 The QoS Monitor Screen 56
7.6 QoS Technical Reference 57
7.6.1 DiffServ 57

Chapter 8
Network Address Translation (NAT) 59

8.1 Overview 59

8.1.1 What You Can Do in this Chapter 59
8.1.2 What You Need To Know 59
8.2 The Port Forwarding Screen 60
8.2.1 The Port Forwarding Screen 61
8.2.2 The Port Forwarding Edit Screen 62
8.3 The DMZ Screen 63
8.4 The Sessions Screen 63
8.5 Technical Reference 64
8.5.1 NAT Definitions 64
8.5.2 What NAT Does 64
8.5.3 How NAT Works 65

Chapter 9
Dynamic DNS 67

9.1 Overview 67
9.1.1 What You Need To Know 67
9.2 The Dynamic DNS Screen 68

Chapter 10
Firewall 69

10.1 Overview 69
10.1.1 What You Can Do in this Chapter 69
10.1.2 What You Need to Know 70
10.2 The General Screen 71
10.3 The Services Screen 72
10.3.1 The Add New Services Entry Screen 72
10.4 The Access Control Screen 73
10.4.1 The Add New ACL Rule/Edit Screen 74
10.5 The DoS Screen 75
10.6 Firewall Technical Reference 76
10.6.1 Guidelines For Enhancing Security With Your Firewall 76
10.6.2 Security Considerations 76

Chapter 11
MAC Filter 79

11.1 Overview 79
11.1.1 What You Need to Know 79
11.2 The MAC Filter Screen 79

Chapter 12
Parental Control 81

12.1 Overview 81
12.2 The Parental Control Screen 81

12.2.1 Add/Edit a Parental Control Rule 82

Chapter 13
VPN 85

13.1 Overview 85
13.2 IPSec VPN 85
13.2.1 The General Screen 85
13.2.2 IPSec VPN: Add 87
13.2.3 The Monitor Screen 91
13.3 Technical Reference 92
13.3.1 IPSec Architecture 92
13.3.2 Encapsulation 93
13.3.3 IKE Phases 94
13.3.4 Negotiation Mode 94
13.3.5 IPSec and NAT 95
13.3.6 VPN, NAT, and NAT Traversal 95
13.3.7 ID Type and Content 96
13.3.8 Pre-Shared Key 97
13.3.9 Diffie-Hellman (DH) Key Groups 98

Chapter 14
Logs 99

14.1 Overview 99
14.1.1 What You Can Do in this Chapter 99
14.1.2 What You Need To Know 99
14.2 The System Log Screen 100

Chapter 15
Traffic Status 101

15.1 Overview 101
15.1.1 What You Can Do in this Chapter 101
15.2 The WAN Status Screen 101
15.3 The LAN Status Screen 102
15.4 The NAT Status Screen 103

Chapter 16
User Account 105

16.1 Overview 105
16.2 The User Account Screen 105

Chapter 17
Remote MGMT....107

17.1 Overview 107

17.1.1 What You Need to Know 107
17.2 The Remote MGMT Screen 107

Chapter 18
System 109

18.1 Overview 109
18.1.1 What You Need to Know 109
18.2 The System Screen 109

Chapter 19
Time Setting 111

19.1 Overview 111
19.2 The Time Setting Screen 111

Chapter 20
Log Setting 113

20.1 Overview 113
20.2 The Log Setting Screen 113

Chapter 21
Firmware Upgrade 115

21.1 Overview 115
21.2 The Firmware Upgrade Screen 115

Chapter 22
Backup/Restore 117

22.1 Overview 117
22.2 The Backup/Restore Screen 117
22.3 The Reboot Screen 119

Chapter 23
Diagnostic 121

23.1 Overview 121
23.2 The Ping/TraceRoute Screen 121

Chapter 24
Troubleshooting 123

24.1 Overview 123
24.2 Power, Hardware Connections, and LEDs 123
24.3 LTE Device Access and Login 124
24.4 Internet Access 125
24.5 UPnP 126

Appendix A IP Addresses and Subnetting 127
Appendix B Setting Up Your Computer's IP Address 137
Appendix C Pop-up Windows, JavaScript and Java Permissions 167
Appendix D Common Services 177
Appendix E Legal Information 181
Index 185

PART I
User's Guide

1 Introduction

1.1 Overview

The Device is an LTE (Long Term Evolution) device including an outdoor unit (ODU) and an indoor unit (IDU). The LTE Device provides a complete security solution with a robust firewall based on Stateful Packet Inspection (SPI) technology and Denial of Service (DoS).

See the chapter on product specifications for a full list of features.

1.2 Applications for the LTE Device

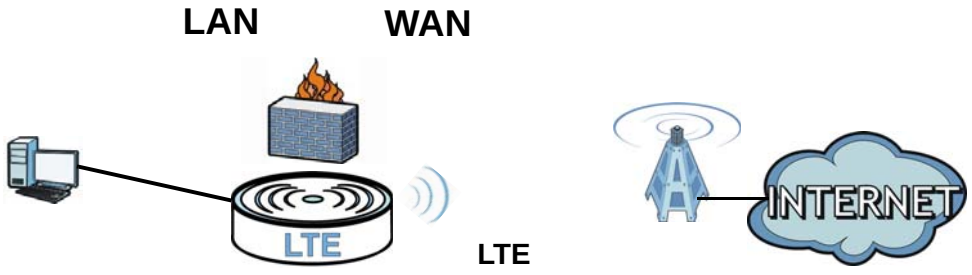
Here are some example uses for which the LTE Device is well suited.

1.2.1 Internet Access

Your LTE Device provides Internet access by connecting to an LTE network wirelessly.

Computers can connect to the LTE Device's **ETHERNET** ports.

Figure 1 LTE Device's Internet Access Application



1.3 Ways to Manage the LTE Device

- Web Configurator. This is for management of the LTE Device using a (supported) web browser.

1.4 Good Habits for Managing the LTE Device

Do the following things regularly to make the LTE Device more secure and to manage the LTE Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password to access the Web Configurator, you will have to reset the LTE Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the LTE Device. You could simply restore your last configuration. Write down any information your ISP provides you.

1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 2 LEDs on the Top of the Device

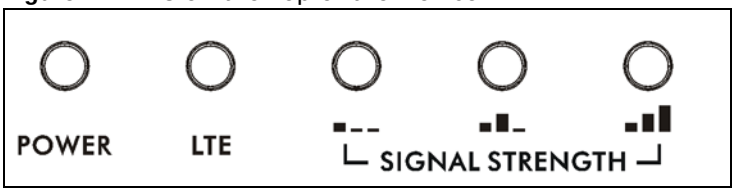
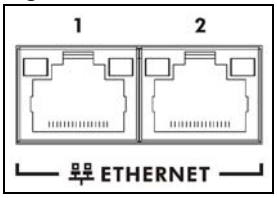


Figure 3 LEDs on the Ethernet Ports



None of the LEDs are on if the LTE Device is not receiving power.

Table 1 LED Descriptions (From Left To Right)

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Green	On	The LTE Device is receiving power and ready for use.
		Blinking	The LTE Device is booting up.
	Red	On	The LTE Device detected an error while self-testing, or there is a device malfunction.
		Blinking	The LTE Device is upgrading the firmware.
	Off		The LTE Device is not receiving power.
LTE	Green	On	The LTE Device has an LTE connection on the WAN.
		Blinking	The LTE Device is searching for a frequency channel or is performing network entry.
	Off		The LTE Device does not have an LTE connection on the WAN.
Signal Strength			The LTE LEDs display the Received Signal Strength Indication (RSSI) of the LTE connection. Three signals on at the same time means best signal quality, two means medium signal quality, and one means low signal quality.
		No Signal LEDS	There is no LTE connection.
	Green	Signal 1 On	The signal strength is less than -90 dBm if signal 1 is on only.
		Signal 2 On	The signal strength is between -90 dBm and -70 dBm if both signals 1 and 2 are on.
		Signal 3 On	The signal strength is -70 dBm or greater if three signals are all on.
ETHERNET1 -2	Yellow (Giga Ethernet)	On	The LTE Device has a successful 1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The LTE Device is sending or receiving data to/from the LAN at 1000 Mbps.
	Green (Fast Ethernet)	On	The LTE Device has a successful 10/100 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The LTE Device is sending or receiving data to/from the LAN at 10/100 Mbps.
	Off		The LTE Device does not have an Ethernet connection with the LAN.

Refer to the Quick Start Guide for information on hardware connections.

1.6 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the passwords will be reset to the defaults.

1 Make sure the **POWER** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for 5 seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

2

Introducing the Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

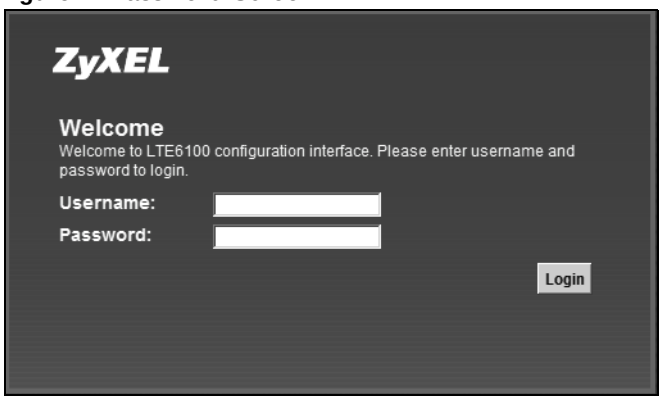
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See Appendix C on page 167 if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

1. Make sure your LTE Device hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. A password screen displays. Type “admin” as the default Username and “1234” as the default password to access the device’s Web Configurator. Click **Login**. If you have changed the password, enter your password and click **Login**.

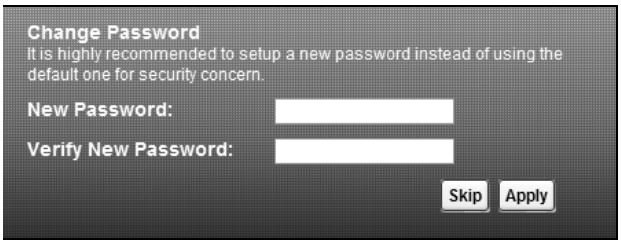
Figure 4 Password Screen



Note: For security reasons, the LTE Device automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Skip** to proceed to the main menu if you do not want to change the password now.

Figure 5 Change Password Screen


Change Password
It is highly recommended to setup a new password instead of using the default one for security concern.
New Password:
Verify New Password:
Skip
Apply

6 The **Connection Status** screen appears.

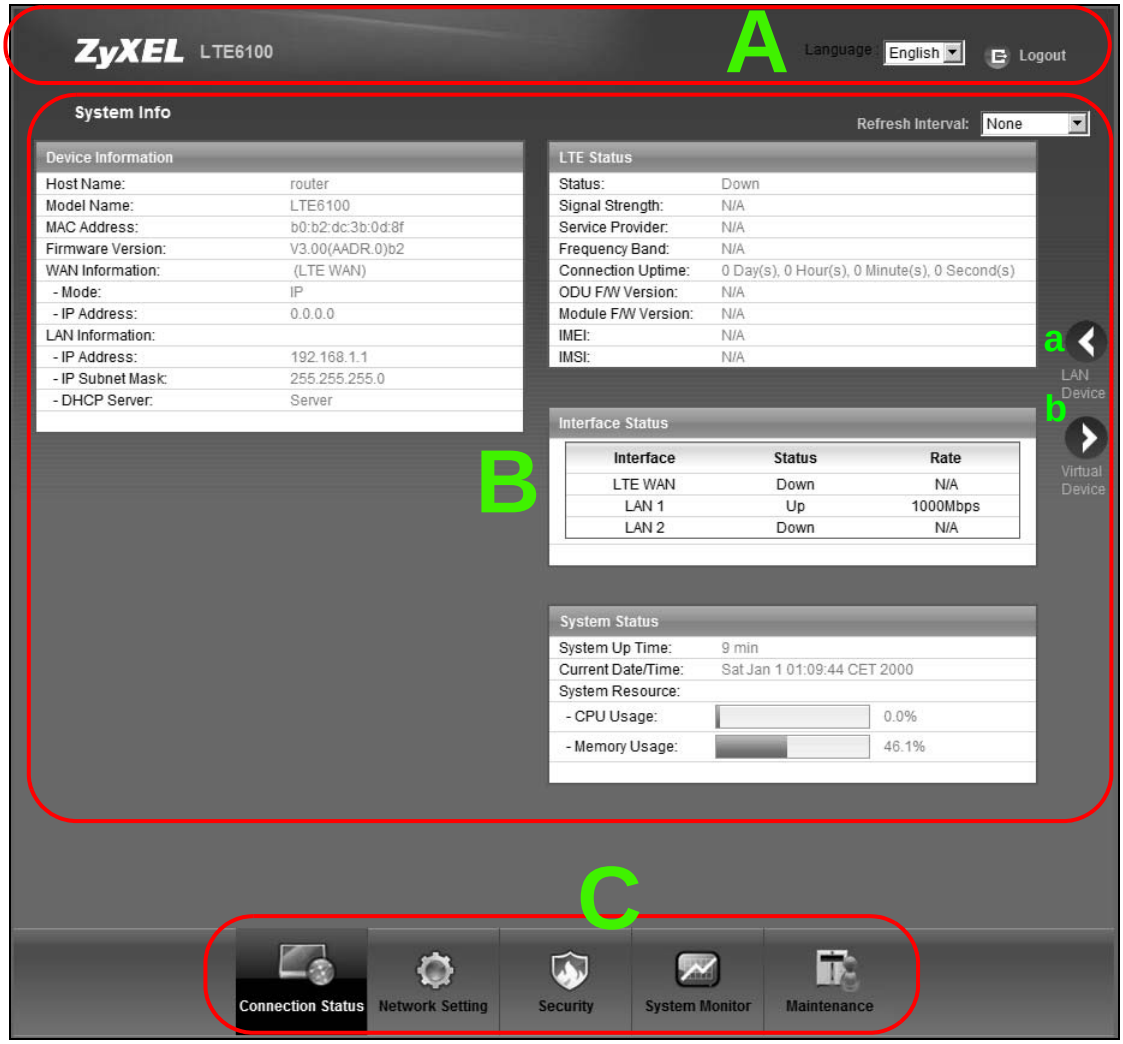
Figure 6 Connection Status

7 Click **System Info** to display the **System Info** screen, where you can view the LTE Device's interface and system information.

2.2 The Web Configurator Layout

Click **Connection Status > System Info** to show the following screen. (See Section 3.3 on page 27 for more information.)

Figure 7 Web Configurator Layout



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - main window
- **C** - navigation panel

2.2.1 Title Bar

The title bar shows the following icon in the upper right corner.

Click this icon to log out of the web configurator.

2.2.2 Main Window

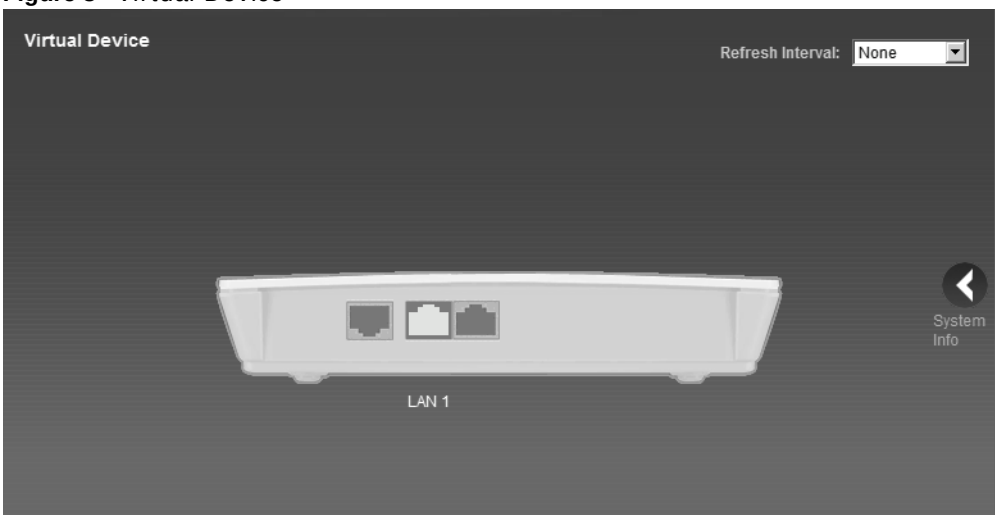
The main window displays information and configuration fields. It is discussed in the rest of this document.

After you click **System Info** on the **Connection Status** screen, the **System Info** screen is displayed. See Chapter 3 on page 27 for more information about the **System Info** screen.

If you click **LAN Device** on the **System Info** screen (**a** in Figure 7 on page 19), the **Connection Status** screen appears. See Chapter 3 on page 25 for more information about the **Connection Status** screen.

If you click **Virtual Device** on the **System Info** screen (**b** in Figure 7 on page 19), a visual graphic appears, showing the connection status of the LTE Device's ports. The connected ports are in color and disconnected ports are gray.

Figure 8 Virtual Device



2.2.3 Traffic Status

Use the **Maintenance > Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT. See Chapter 18 on page 109 for more information.

2.2.4 User Account

Use the **Maintenance > User Accounts** screen to configure system password for different user accounts. See Chapter 16 on page 105 for more information.

2.2.5 Navigation Panel

Use the menu items on the navigation panel to open screens to configure LTE Device features. The following table describes each menu item.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the LTE Device and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and modify your WAN interface.
	SIM	Use this screen to enter the PIN of your SIM card.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to enable the UPnP function.
Static Route	Static Route	Use this screen to view and set up static routes on the LTE Device.
QoS	General	Use this screen to enable QoS and decide allowable bandwidth using QoS.
	Queue Setup	Use this screen to configure QoS queue assignment.
	Class Setup	Use this screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.
	Monitor	Use this screen to view each queue's statistics.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	DMZ	Use this screen to configure the IP address of the LTE Device's DMZ interface.
	Sessions	Use this screen to limit the number of NAT sessions a single client can establish.
Dynamic DNS	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	Use this screen to view and configure services.
	Access Control	Use this screen to view and configure filter rules for incoming and outgoing traffic.
	DoS	Use this screen to activate/deactivate Denial of Service (DoS) protection.
MAC Filter	MAC Filter	Use this screen to allow specific devices to access the LTE Device.
Parental Control	Parental Control	Use this screen to define time periods and days during which the LTE Device performs parental control and/or block web sites with the specific URL.
VPN	Setup	Use this screen to configure IPSec VPN connections.
	Monitor	Use this screen to view IPSec VPN connection status.
System Monitor		
Log	System Log	Use this screen to view the system logs for the categories that you select.

Table 2 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the LTE Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the LTE Device.
	NAT	Use this screen to view the status of NAT sessions on the LTE Device.
Maintenance		
Users Account	Users Account	Use this screen to configure the passwords your user accounts.
Remote MGMT	Remote MGMT	Use this screen to enable specific traffic directions for network services.
System	System	Use this screen to configure the LTE Device's name, domain name, management inactivity time-out.
Time Setting	Time Setting	Use this screen to change your LTE Device's time and date.
Log Setting	Log Setting	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your device.
Backup/ Restore	Backup/Restore	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the LTE Device without turning the power off.
Diagnostic	Ping/TraceRoute	Use this screen to test the connections to other devices.

PART II
Technical Reference

The appendices provide general information. Some details may not apply to your LTE Device.

3

Connection Status and System Info

3.1 Overview

After you log into the web configurator, the **Connection Status** screen appears. This shows the network connection status of the LTE Device and clients connected to it.

Use the **System Info** screen to look at the current status of the device, system resources, interfaces (LAN, WAN).

If you click **Virtual Device** on the **System Info** screen, a visual graphic appears, showing the connection status of the LTE Device's ports. See Section 2.2.2 on page 20 for more information.

3.2 The Connection Status Screen

Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem.

If you prefer to view the status in a list, click **List View** in the **Viewing mode** selection box. You can configure how often you want the LTE Device to update this screen in **Refresh Interval**.

Figure 9 Connection Status: Icon View

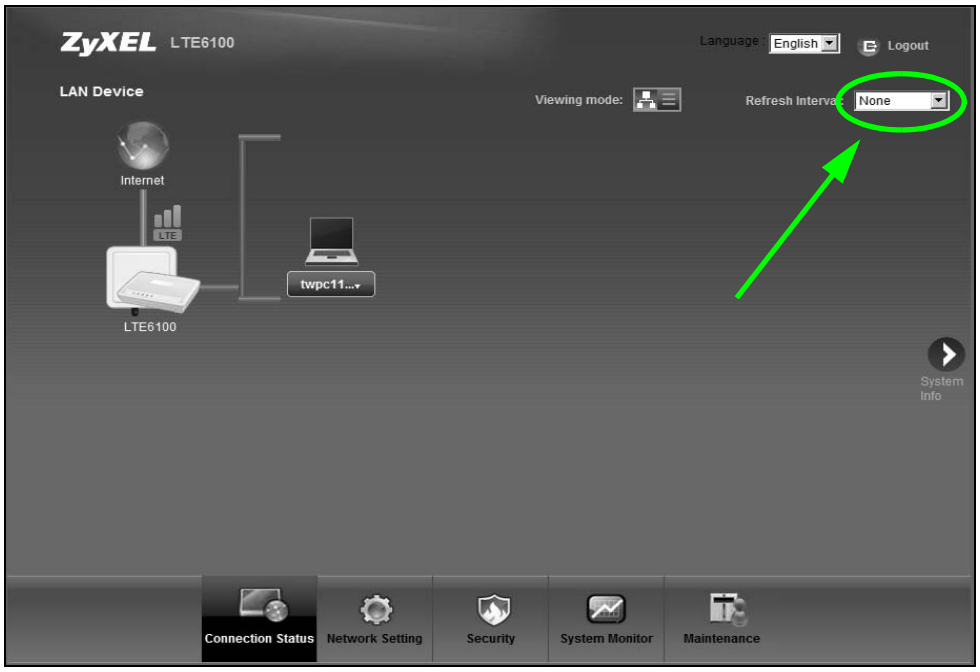
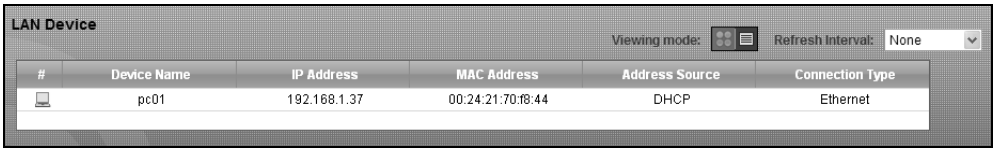


Figure 10 Connection Status: List View



In **Icon View**, if you want to view information about a client, click the client's name and **Info**. Click the IP address if you want to change it. If you want to change the name or icon of the client, click **Change name/icon**.

In **List View**, you can also view the client's information.

3.3 The System Info Screen

Click **Connection Status > System Info** to open this screen.

Figure 11 System Info Screen

Each field is described in the following table.

Table 3 System Info Screen

LABEL	DESCRIPTION
Language	Select the web configurator language from the drop-down list box.
Refresh Interval	Select how often you want the LTE Device to update this screen from the drop-down list box.
Device Information	
Host Name	This field displays the LTE Device system name. It is used for identification. You can change this in the **Maintenance > System** screen's **Host Name** field.
Model Name	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your LTE Device.
Software Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Go to the **Maintenance > Firmware Upgrade** screen to change it.
WAN Information	

Table 3 System Info Screen (continued)

LABEL	DESCRIPTION
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the LTE Device in the WAN.
LAN Information	
IP Address	This field displays the current IP address of the LTE Device in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP Server	This field displays what DHCP services the LTE Device is providing to the LAN. Choices are: **Server** - The LTE Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **None** - The LTE Device is not providing any DHCP services to the LAN.
LTE Status	
Status	This displays **4G LTE** if there is an LTE connection, otherwise, it displays **N/A**.
Signal Strength	This displays the strength of the LTE connection that the LTE Device has with the base station which is also known as eNodeB or eNB.
Service Provider	This displays the service provider's name of the connected LTE network.
Frequency Band	This displays **LTE** if there is an LTE connection.
Connection Uptime	This displays how long the LTE connection has been available since it was last established successfully.
ODU F/W Version	This displays the firmware version of the outdoor unit.
Module F/W Version	This displays the firmware version of LTE module.
IMEI	This displays the LTE Device's International Mobile Equipment Identity number (IMEI). An IMEI is a unique ID used to identify a mobile device.
IMSI	This displays the International Mobile Subscriber Identity (IMSI) of the SIM card inserted in the outdoor unit. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
Interface Status	
Interface	This column displays each interface the LTE Device has.
Status	This field indicates whether or not the LTE Device is using the interface. For the LTE WAN interface, this field displays **Up** when the LTE Device is connected to an LTE network and **Down** when the LTE Device does not have an LTE connection. For the LAN interface, this field displays **Up** when the LTE Device is using the interface and **Down** when the LTE Device is not using the interface.
Rate	For the LTE WAN interface, this displays **4G LTE** if there is an LTE connection. For the LAN interface, this displays the port speed and duplex setting.
System Status	
System Up Time	This field displays how long the LTE Device has been running since it last started up. The LTE Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it (see Section 1.6 on page 15).
Current Date/Time	This field displays the current date and time in the LTE Device. You can change this in **Maintenance > Time Setting**.
System Resource	

Table 3 System Info Screen (continued)

LABEL	DESCRIPTION
CPU Usage	This field displays what percentage of the LTE Device's processing ability is currently used. When this percentage is close to 100%, the LTE Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
Memory Usage	This field displays what percentage of the LTE Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the LTE Device is probably becoming unstable, and you should restart the device. See Chapter 22 on page 119, or turn off the device (unplug the power) for a few seconds.

4

Broadband

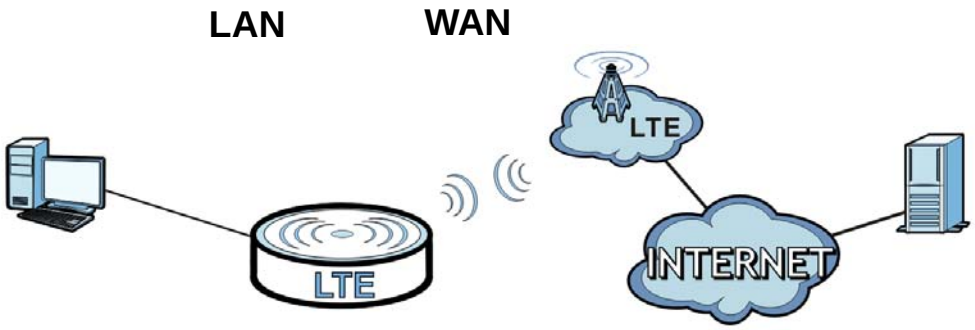
4.1 Overview

This chapter discusses the LTE Device's **Broadband** screens. Use these screens to configure your LTE Device for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

This LTE Device supports LTE connection for the WAN only.

Figure 12 LAN and WAN



4.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view or edit an LTE WAN interface. You can also configure the WAN settings on the LTE Device for Internet access (Section 4.2 on page 32).
- Use the **SIM** screen to enter the PIN of your SIM card (Section 4.3 on page 33).

4.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

WAN IP Address

The WAN IP address is an IP address for the LTE Device, which makes it accessible from an outside network. It is used by the LTE Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the LTE Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

APN

Access Point Name (APN) is a unique string which indicates an LTE network. An APN is required for LTE stations to enter the LTE network and then the Internet.

4.1.3 Before You Begin

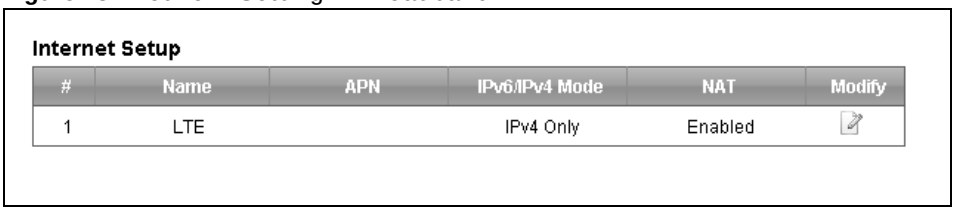
You may need to know your Internet access settings such as LTE APN, WAN IP address and SIM card's PIN code if the **INTERNET** light on your LTE Device is off. Get this information from your service provider.

4.2 The Broadband Screen

The LTE Device must have a WAN interface to allow users to use the LTE connection to access the Internet. Use the **Broadband** screen to view or modify a WAN interface.

Click **Network Setting > Broadband**. The following screen opens.

Figure 13 Network Setting > Broadband



The following table describes the fields in this screen.

Table 4 Network Setting > Broadband

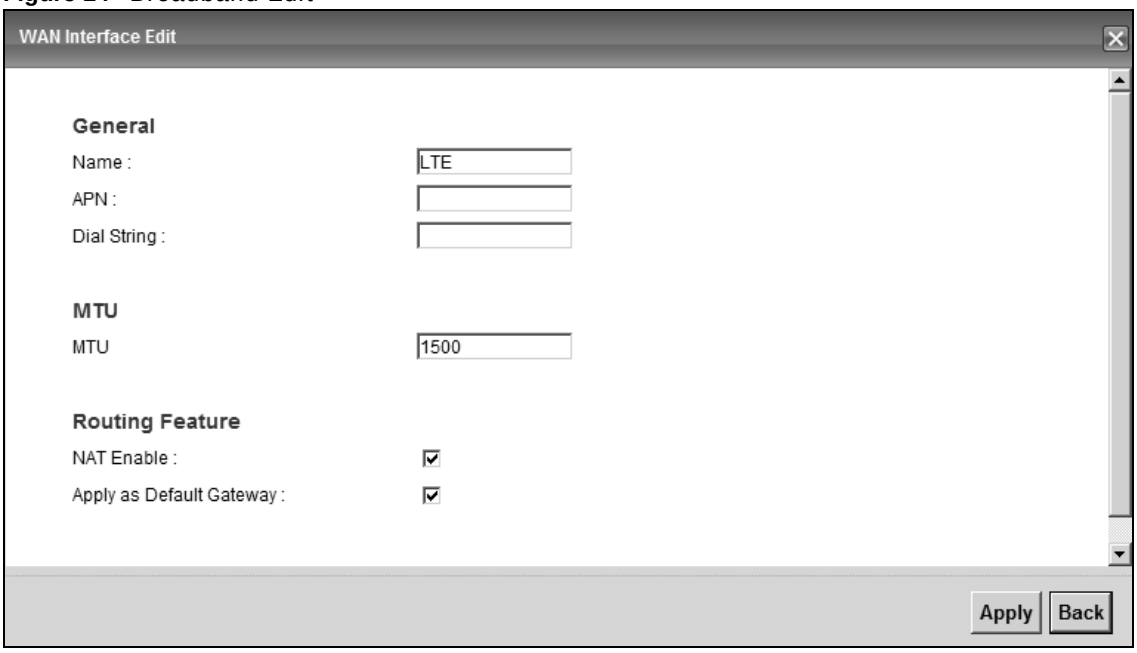
LABEL	DESCRIPTION
Internet Setup	
Name	This is the service name of the connection.
APN	This is the name of the LTE network to which the LTE Device will connect.
IPv6/IPv4 Mode	This shows whether the connection uses IPv6 or IPv4.
NAT	This shows whether NAT is activated or not for this connection. NAT is not available when the connection uses the bridging service.
Modify	Click the **Edit** icon to configure the connection. Click the **Delete** icon to delete this connection from the Device. A window displays asking you to confirm that you want to delete the connection.

4.2.1 Edit Internet Connection

Use this screen to configure a WAN connection.

Click the **Edit** icon next to the LTE connection, the screen displays as shown next.

Figure 14 Broadband Edit



The following table describes the fields in this screen.

Table 5 Broadband Edit

LABEL	DESCRIPTION
Name	Specify the name for this WAN interface.
APN	Enter the Access Point Name (APN) of an LTE network, which your service provider gave you.
Dial String	Enter the dial string for the ISP.
MTU	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU for this WAN interface in this field.
NAT Enable	Select this to activate NAT on the WAN.
Apply as Default Gateway	Select this option to have the LTE Device use the WAN interface of this connection as the system default gateway.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

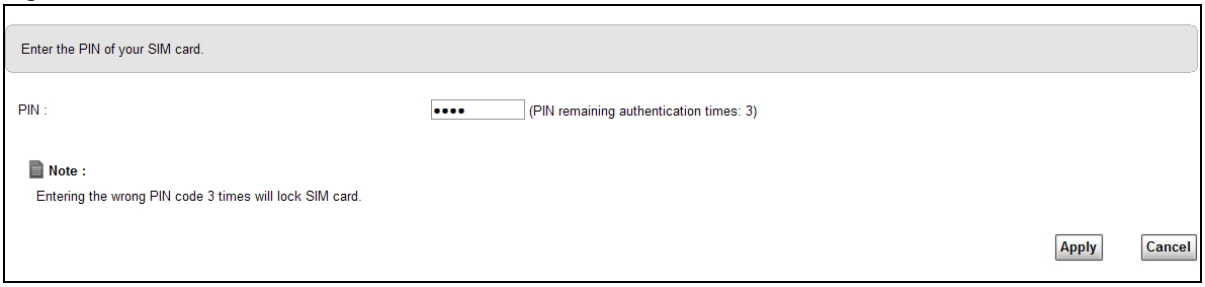
4.3 The SIM Screen

Use the **SIM** screen to enter the PIN of your SIM card.

If the wrong PIN code is entered 3 times, it will cause the SIM card to be locked.

Click **Network Setting > Broadband > SIM**. The following screen opens.

Figure 15 SIM


Enter the PIN of your SIM card.
PIN :
(PIN remaining authentication times: 3)
Note :
Entering the wrong PIN code 3 times will lock SIM card.
Apply
Cancel

The following table describes the fields in this screen.

Table 6 SIM

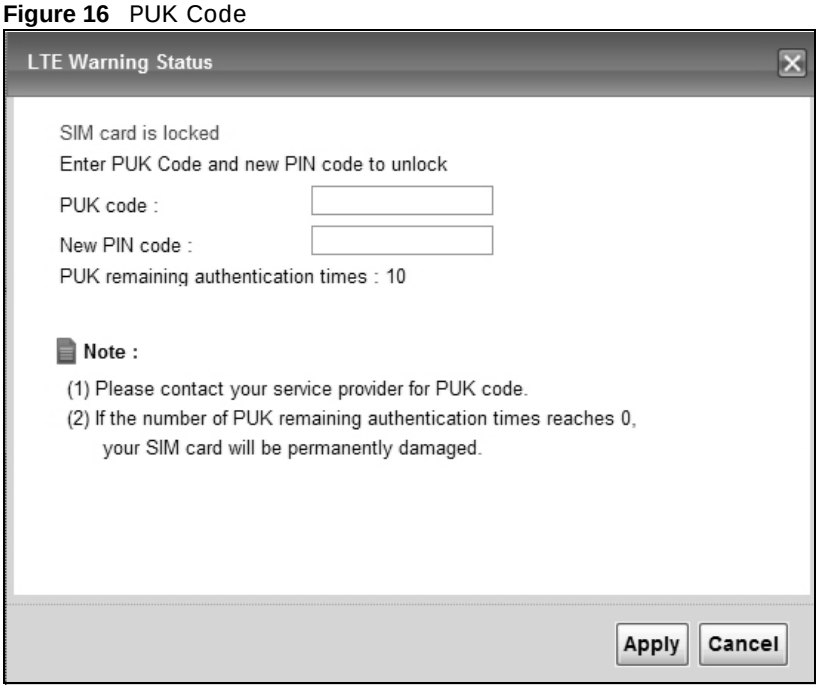
LABEL	DESCRIPTION
PIN	Enter the PIN of your SIM card.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return to the previous screen without saving.

4.3.1 PUK Code Screen

If the SIM card is locked, use this screen to enter the PUK code.

Note: You may have to ask the service provider for a PUK code to unlock the SIM card.

Figure 16 PUK Code


LTE Warning Status
SIM card is locked
Enter PUK Code and new PIN code to unlock
PUK code :
New PIN code :
PUK remaining authentication times : 10
Note :
(1) Please contact your service provider for PUK code.
(2) If the number of PUK remaining authentication times reaches 0,
your SIM card will be permanently damaged.
Apply
Cancel

The following table describes the fields in this screen.

Table 7 PUK Code

LABEL	DESCRIPTION
PUK code	Enter the PUK (Pin Unlock Key) code to unlock the SIM card.
New PIN code	Enter the new PIN code for the SIM card.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return to the previous screen without saving.

4.4 Technical Reference

The following section contains additional technical information about the LTE Device features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The LTE Device supports the following methods:

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The LTE Device can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2 If your ISP dynamically assigns the DNS server IP addresses (along with the LTE Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

LTE Frequency Band Table

See the following table for the frequency bands used in LTE wireless technologies.

Table 8 LTE Wireless Technologies

BAND	UPLINK (UL) OPERATING BAND BASE STATION RECEIVE CPE TRANSMIT	DOWNLINK (DL) OPERATING BAND BASE STATION TRANSMIT CPE RECEIVE	DUPLEX MODE
	UL (LOW - HIGH)	DL (LOW - HIGH)	
1	1920 MHz – 1980 MHz	2110 MHz – 2170 MHz	FDD
2	1850 MHz – 1910 MHz	1930 MHz – 1990 MHz	FDD
3	1710 MHz – 1785 MHz	1805 MHz – 1880 MHz	FDD
4	1710 MHz – 1755 MHz	2110 MHz – 2155 MHz	FDD
5	824 MHz – 849 MHz	869 MHz – 894MHz	FDD
6	830 MHz – 840 MHz	875 MHz – 885 MHz	FDD
7	2500 MHz – 2570 MHz	2620 MHz – 2690 MHz	FDD
8	880 MHz – 915 MHz	925 MHz – 960 MHz	FDD
9	1749.9 MHz – 1784.9 MHz	1844.9 MHz – 1879.9 MHz	FDD
10	1710 MHz – 1770 MHz	2110 MHz – 2170 MHz	FDD
11	1427.9 MHz – 1447.9 MHz	1475.9 MHz – 1495.9 MHz	FDD
12	699 MHz – 716 MHz	729 MHz – 746 MHz	FDD
13	777 MHz – 787 MHz	746 MHz – 756 MHz	FDD
14	788 MHz – 798 MHz	758 MHz – 768 MHz	FDD
15	Reserved	Reserved	FDD
16	Reserved	Reserved	FDD
17	704 MHz – 716 MHz	734 MHz – 746 MHz	FDD
18	815 MHz – 830 MHz	860 MHz – 875 MHz	FDD
19	830 MHz – 845 MHz	875 MHz – 890 MHz	FDD
20	832 MHz – 862 MHz	791 MHz – 821 MHz	FDD
21	1447.9 MHz – 1462.9 MHz	1495.9 MHz – 1510.9 MHz	FDD
...			
24	1626.5 MHz – 1660.5 MHz	1525 MHz – 1559 MHz	FDD
...			
33	1900 MHz – 1920 MHz	1900 MHz – 1920 MHz	TDD
34	2010 MHz – 2025 MHz	2010 MHz – 2025 MHz	TDD
35	1850 MHz – 1910 MHz	1850 MHz – 1910 MHz	TDD
36	1930 MHz – 1990 MHz	1930 MHz – 1990 MHz	TDD
37	1910 MHz – 1930 MHz	1910 MHz – 1930 MHz	TDD
38	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz	TDD
39	1880 MHz – 1920 MHz	1880 MHz – 1920 MHz	TDD
40	2300 MHz – 2400 MHz	2300 MHz – 2400 MHz	TDD
41	2496 MHz 2690 MHz	2496 MHz 2690 MHz	TDD
42	3400 MHz – 3600 MHz	3400 MHz – 3600 MHz	TDD

Table 8 LTE Wireless Technologies (continued)

BAND	UPLINK (UL) OPERATING BAND BASE STATION RECEIVE CPE TRANSMIT	DOWNLINK (DL) OPERATING BAND BASE STATION TRANSMIT CPE RECEIVE	DUPLEX MODE
	UL (LOW - HIGH)	DL (LOW - HIGH)	
43	3600 MHz – 3800 MHz	3600 MHz – 3800 MHz	TDD
Note 1: Band 6 is not applicable			

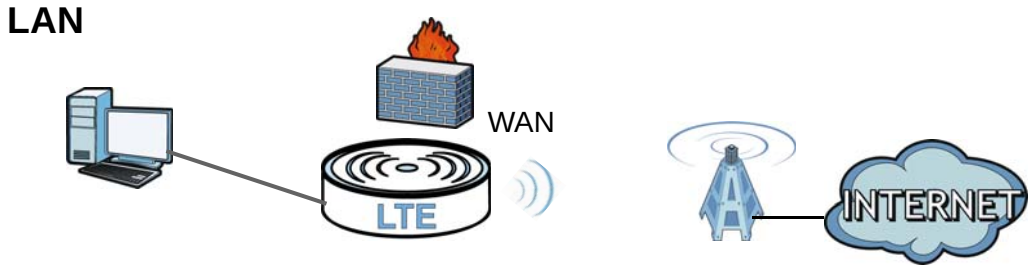
5

Home Networking

5.1 Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.



5.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, DHCP, subnet mask, and DNS settings (Section 5.2 on page 41).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 5.3 on page 42).
- Use the **UPnP** screen to enable UPnP (Section 5.4 on page 43).

5.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

5.1.2.1 About LAN

IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your LTE Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the LTE Device unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This LTE Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

5.1.2.2 About UPnP

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

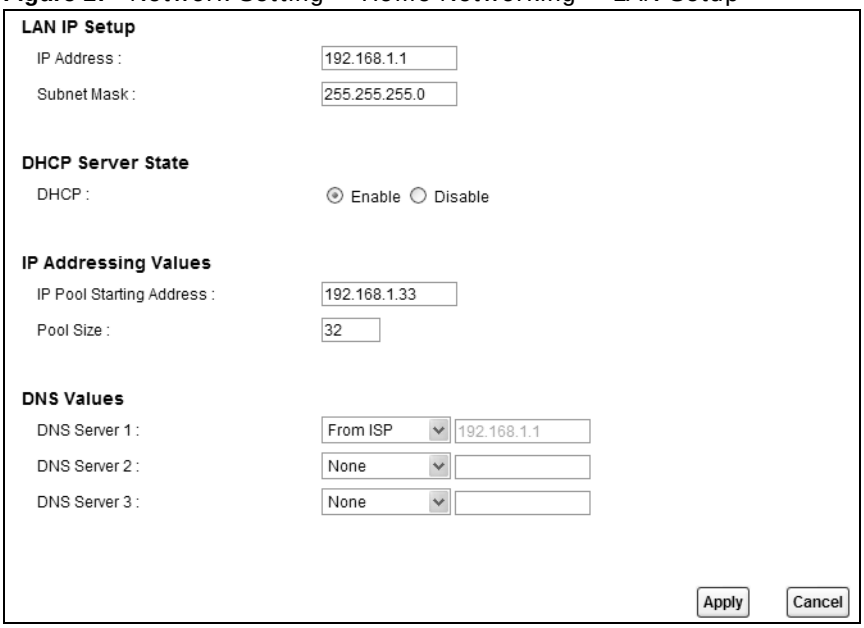
When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the LTE Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

5.2 The LAN Setup Screen

Click **Network Setting > Home Networking** to open the **LAN Setup** screen. Use this screen to set the Local Area Network IP address and subnet mask of your LTE Device and configure the DNS server information that the LTE Device sends to the DHCP client devices on the LAN.

Figure 17 Network Setting > Home Networking > LAN Setup



The following table describes the fields in this screen.

Table 9 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your LTE Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your LTE Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	
DHCP	Select **Enable** to have your LTE Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN. When DHCP is used, the following fields need to be set.
IP Addressing Values	
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DNS Values	

Table 9 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DNS Server 1-3	Select **From ISP** if your ISP dynamically assigns DNS server information (and the LTE Device's WAN IP address). Select **DNS-Proxy** to have the LTE Device send its own address to the LAN clients for them to use as the DNS server. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

5.3 The Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

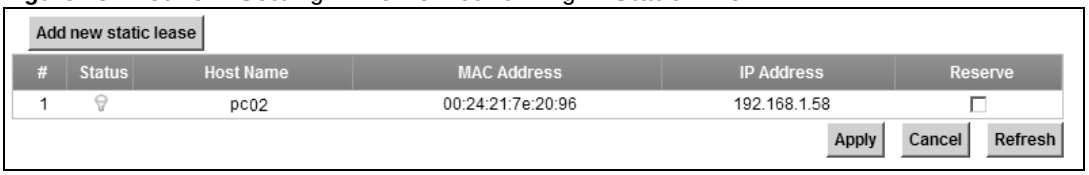
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

5.3.1 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the **Static DHCP** screen.

Use this screen to change your LTE Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 18 Network Setting > Home Networking > Static DHCP



The following table describes the labels in this screen.

Table 10 Network Setting > Home Networking > Static DHCP

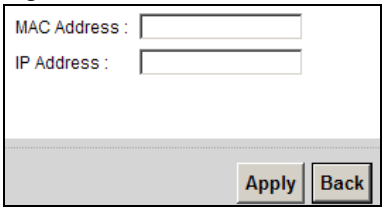
LABEL	DESCRIPTION
Add new static lease	Click this to add a new static DHCP entry.
#	This is the index number of the entry.

Table 10 Network Setting > Home Networking > Static DHCP (continued)

LABEL	DESCRIPTION
Status	This field displays whether the client is connected to the LTE Device.
Host Name	This field displays the client host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the LTE Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.
Refresh	Click **Refresh** to reload the DHCP table.

If you click **Add new static lease** in the **Static DHCP** screen, the following screen displays.

Figure 19 Static DHCP: Add



The following table describes the labels in this screen.

Table 11 Static DHCP: Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of a computer on your LAN.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

5.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

Use the following screen to configure the UPnP settings on your LTE Device. Click **Network Setting > Home Networking > Static DHCP > UPnP** to display the screen shown next.

Figure 20 Network Setting > Home Networking > UPnP

The following table describes the labels in this screen.

Table 12 Network Settings > Home Networking > UPnP

LABEL	DESCRIPTION
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the LTE Device's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save your changes.

6

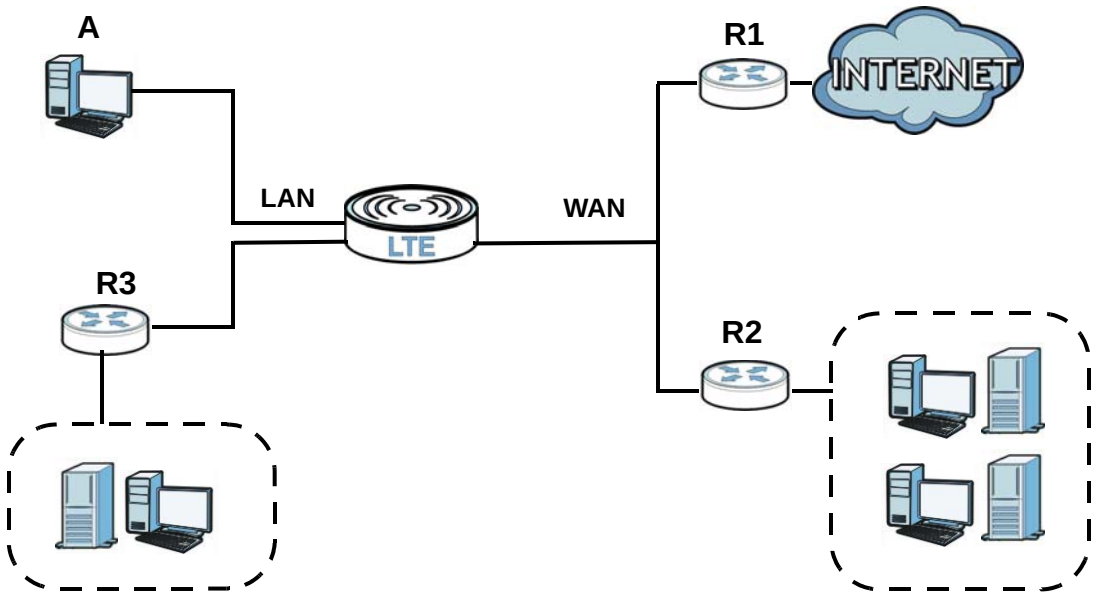
Routing

6.1 Overview

The LTE Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the LTE Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the LTE Device's LAN interface. The LTE Device routes most traffic from **A** to the Internet through the LTE Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 21 Example of Static Routing Topology



6.2 Configuring Static Route

Use this screen to view and configure IP static routes on the LTE Device. Click **Network Setting > Static Route** to open the following screen.

Figure 22 Network Setting > Static Route

The following table describes the labels in this screen.

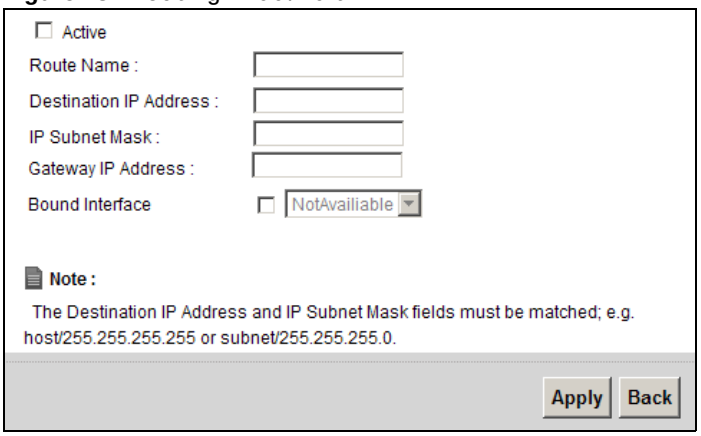
Table 13 Network Setting > Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the LTE Device.
#	This is the number of an individual static route.
Active	This indicates whether the rule is active or not. A yellow bulb signifies that this static route is active. A gray bulb signifies that this static route is not active.
Status	This shows whether the static route is currently in use or not. A yellow bulb signifies that this static route is in use. A gray bulb signifies that this static route is not in use.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Interface	This indicates which interface handles the traffic forwarded by this route.
Modify	Click the **Edit** icon to go to the screen where you can set up a static route on the LTE Device. Click the **Delete** icon to remove a static route from the LTE Device.

6.2.1 Add/Edit Static Route

Click **add new Static Route** in the **Routing** screen or click the **Edit** icon next to a rule. The following screen appears. Use this screen to configure the required information for a static route.

Figure 23 Routing: Add/Edit



The following table describes the labels in this screen.

Table 14 Routing: Add/Edit

LABEL	DESCRIPTION
Active	Click this to activate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure **Gateway IP Address**, enter the IP address of the next-hop gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Bound Interface	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure **Bound Interface**, select the check box and choose an interface through which the traffic is sent.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

7

Quality of Service (QoS)

7.1 Overview

This chapter discusses the LTE Device's **QoS** screens. Use these screens to set up your LTE Device to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. QoS allows the LTE Device to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

The LTE Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

7.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable QoS, set the bandwidth, and allow the LTE Device to automatically assign priority to upstream traffic according to the IP precedence or packet length (Section 7.2 on page 50).
- Use the **Queue Setup** screen to configure QoS queue assignment (Section 7.3 on page 51).
- Use the **Class Setup** screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow (Section 7.4 on page 52).
- Use the **Monitor** screen to view the LTE Device's QoS-related packet statistics (Section 7.5 on page 56).

7.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technology includes DiffServ (Differentiated Services or DS). DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

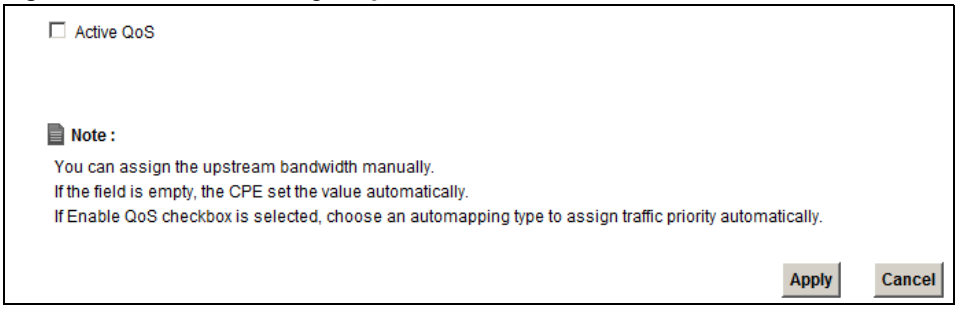
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

7.2 The QoS General Screen

Use this screen to enable or disable QoS, set the bandwidth, and select to have the LTE Device automatically assign priority to upstream traffic according to the IP precedence or packet length.

Click **Network Setting > QoS** to open the **General** screen.

Figure 24 Network Setting > QoS > General


Active QoS
Note :
You can assign the upstream bandwidth manually.
If the field is empty, the CPE set the value automatically.
If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.
Apply
Cancel

The following table describes the labels in this screen.

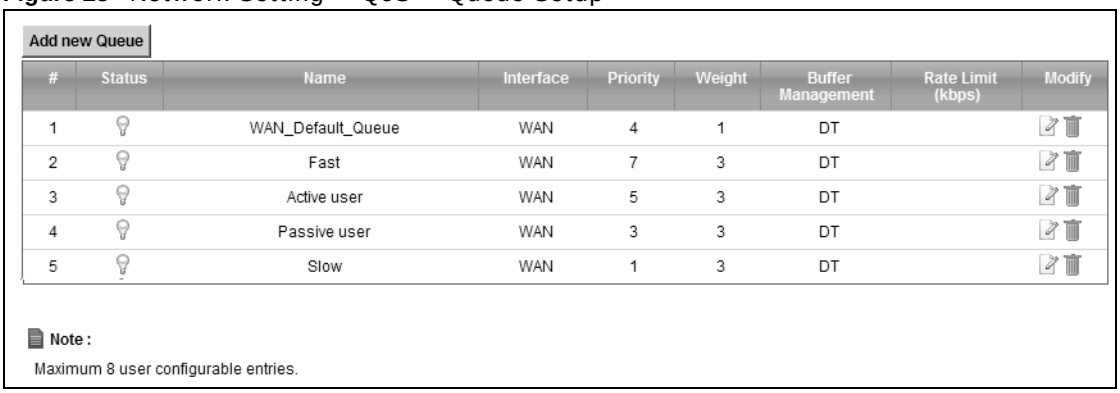
Table 15 Network Setting > QoS > General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the LTE Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.3 The Queue Setup Screen

Use this screen to configure QoS queue assignment. Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Figure 25 Network Setting > QoS > Queue Setup


Add new Queue
Status Name Interface Priority Weight Buffer Management Rate Limit (kbps) Modify
1 WAN_Default_Queue WAN 4 1 DT
2 Fast WAN 7 3 DT
3 Active user WAN 5 3 DT
4 Passive user WAN 3 3 DT
5 Slow WAN 1 3 DT
Note :
Maximum 8 user configurable entries.

The following table describes the labels in this screen.

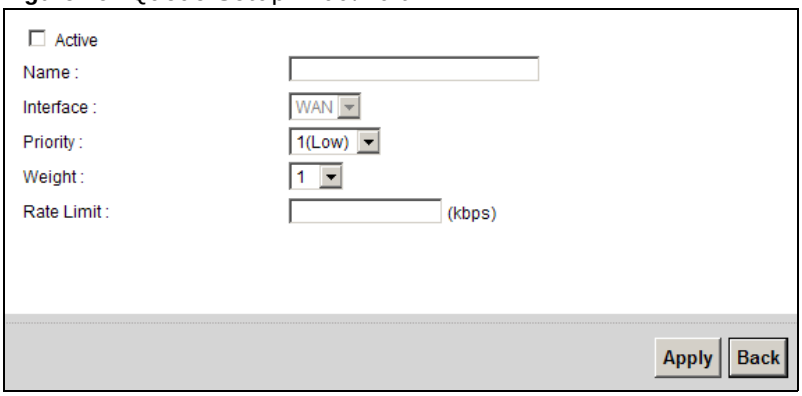
Table 16 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add new Queue	Click this to create a new entry.
#	This is the index number of this entry.
Status	This indicates whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the LTE Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used by the LTE Device.
Rate Limit (kbps)	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

7.3.1 Add/Edit a QoS Queue

Use this screen to configure a queue. Click **Add new Queue** in the **Queue Setup** screen or the **Edit** icon next to an existing queue.

Figure 26 Queue Setup: Add/Edit



The following table describes the labels in this screen.

Table 17 Queue Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	This shows the interface of this queue.
Priority	Select the priority level (from 1 to 7) of this queue. The larger the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 15) of this queue. If two queues have the same priority level, the LTE Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

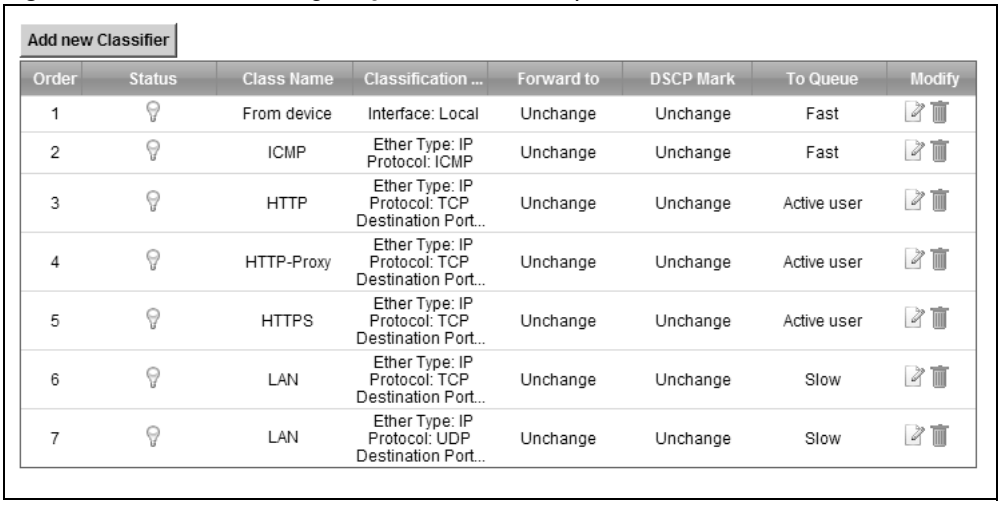
7.4 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the LTE Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Class Setup** to open the following screen.

Figure 27 Network Setting > QoS > Class Setup


Add new Classifier
Order
Status
Class Name
Classification ...
Forward to
DSCP Mark
To Queue
Modify
1 From device Interface: Local Unchange Unchange Fast
2 ICMP Ether Type: IP Protocol: ICMP Unchange Unchange Fast
3 HTTP Ether Type: IP Protocol: TCP Destination Port... Unchange Unchange Active user
4 HTTP-Proxy Ether Type: IP Protocol: TCP Destination Port... Unchange Unchange Active user
5 HTTPS Ether Type: IP Protocol: TCP Destination Port... Unchange Unchange Active user
6 LAN Ether Type: IP Protocol: TCP Destination Port... Unchange Unchange Slow
7 LAN Ether Type: IP Protocol: UDP Destination Port... Unchange Unchange Slow

The following table describes the labels in this screen.

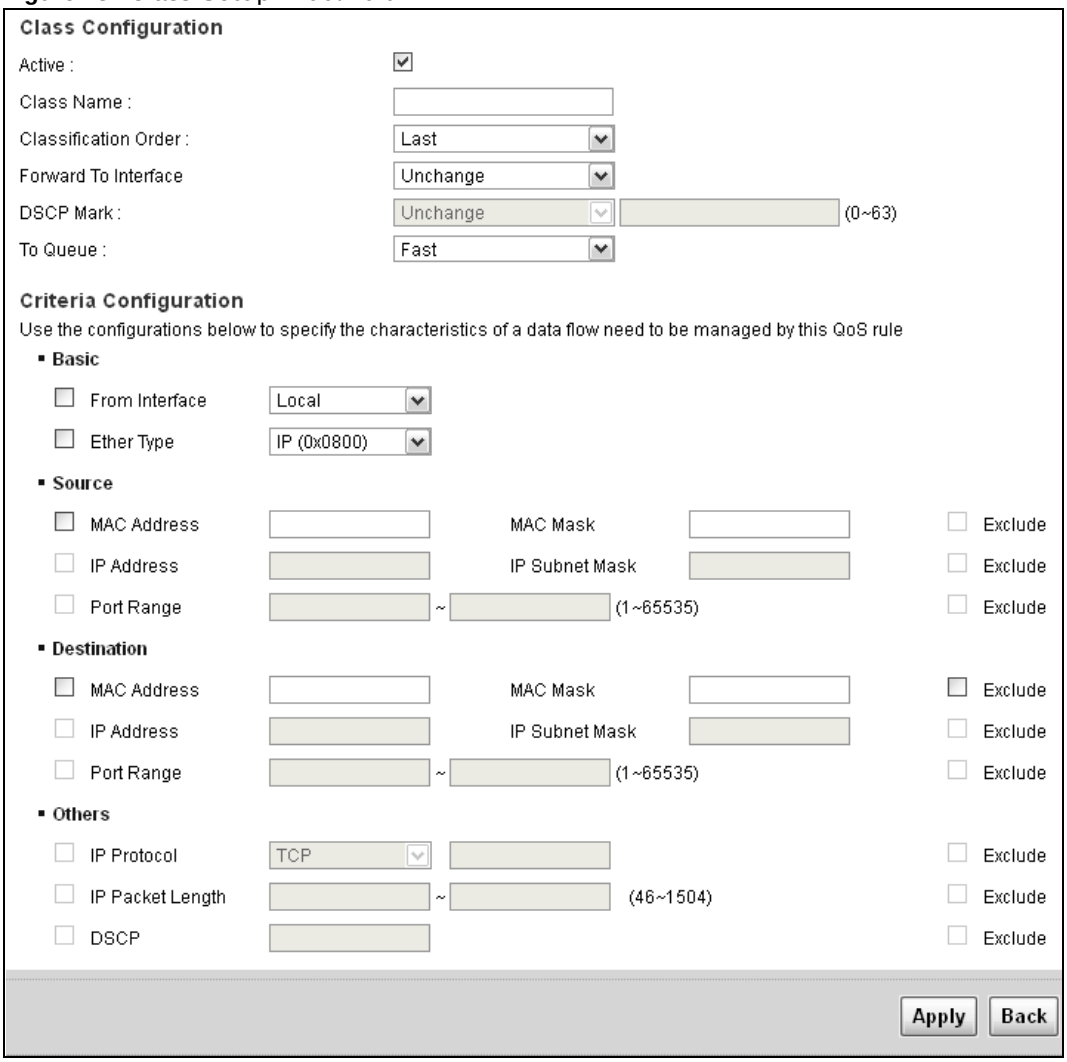
Table 18 Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
Order	This field displays the order number of the classifier.
Status	This indicates whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
Forward to	This is the interface through which traffic that matches this classifier is forwarded out.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to edit the classifier. Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

7.4.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to an existing classifier to configure it.

Figure 28 Class Setup: Add/Edit



The following table describes the labels in this screen.

Table 19 Class Setup: Add/Edit

LABEL	DESCRIPTION
Class Configuration	
Active	Select to enable this classifier.
Class Name	Enter a descriptive name of up to 32 printable English keyboard characters, including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.

Table 19 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the LTE Device forward traffic of this class according to the default routing table.
DSCP Mark	This field is available only when you select the **Ether Type** check box in **Criteria Configuration-Basic** section. If you select **Mark**, enter a DSCP value with which the LTE Device replaces the DSCP field in the packets. If you select **Unchange**, the LTE Device keep the DSCP field in the packets.
To Queue	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Criteria Configuration Use the following fields to configure the criteria for traffic classification.	
Basic	
From Interface	Select whether the traffic class comes from the **LTE**, **Local**, or **Lan** interface.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type.
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.

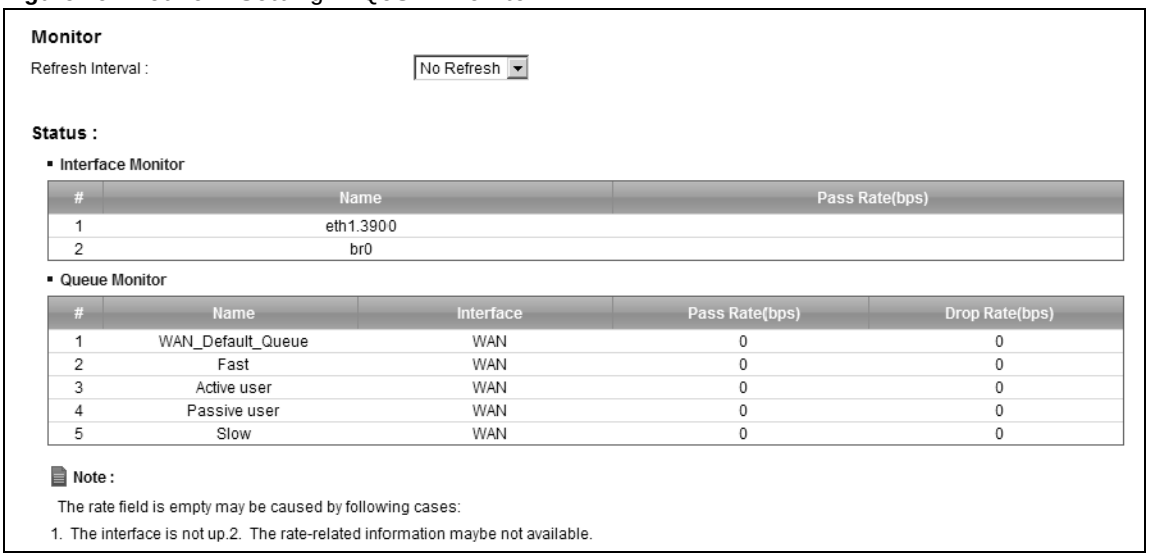
Table 19 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP** or **UDP**. If you select **User defined**, enter the protocol (service type) number.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1504) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

7.5 The QoS Monitor Screen

To view the LTE Device's QoS packet statistics, click **Network Setting > QoS > Monitor**. The screen appears as shown.

Figure 29 Network Setting > QoS > Monitor


Monitor
Refresh Interval :
No Refresh
Status :
Interface Monitor
Name Pass Rate(bps)
1 eth1.3900
2 br0
Queue Monitor
Name Interface Pass Rate(bps) Drop Rate(bps)
1 WAN_Default_Queue WAN 0 0
2 Fast WAN 0 0
3 Active user WAN 0 0
4 Passive user WAN 0 0
5 Slow WAN 0 0
Note :
The rate field is empty may be caused by following cases:
1. The interface is not up.2. The rate-related information maybe not available.

The following table describes the labels in this screen.

Table 20 Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Monitor	
Refresh Interval	Select how often you want the LTE Device to update this screen. Select **No Refresh** to stop refreshing statistics.
Status	
#	This is the index number of the entry.
Name	This shows the name of the WAN interface on the LTE Device.
Pass Rate (bps)	This shows how much traffic (bps) forwarded to this interface are transmitted successfully.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate (bps)	This shows how much traffic (bps) assigned to this queue are transmitted successfully.
Drop Rate (bps)	This shows how much traffic (bps) assigned to this queue are dropped.

7.6 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

7.6.1 DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

8

Network Address Translation (NAT)

8.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 8.2 on page 60).
- Use the **DMZ** screen to view and configure the IP address of your network DMZ. (Section 8.3 on page 63).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use (Section 8.4 on page 63).

8.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Inside/Outside and Global/Local

Inside/outside denotes where a host is located relative to the LTE Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See Section 8.5 on page 64 for advanced technical information on NAT.

8.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

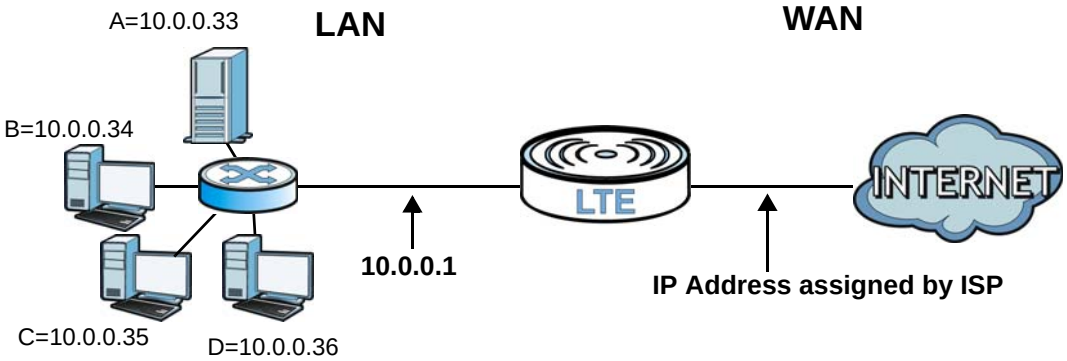
The most often used port numbers and services are shown in Appendix D on page 177. Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 10.0.0.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 30 Multiple Servers Behind NAT Example

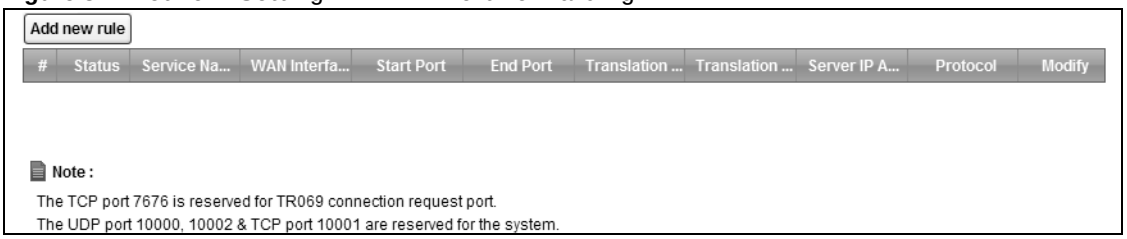


8.2.1 The Port Forwarding Screen

Click **Network Setting > NAT** to open the **Port Forwarding** screen.

See Appendix D on page 177 for port numbers commonly used for particular services.

Figure 31 Network Setting > NAT > Port Forwarding


Add new rule
Status Service Na... WAN Interfa... Start Port End Port Translation ... Translation ... Server IP A... Protocol Modify
Note :
The TCP port 7676 is reserved for TR069 connection request port.
The UDP port 10000, 10002 & TCP port 10001 are reserved for the system.

The following table describes the fields in this screen.

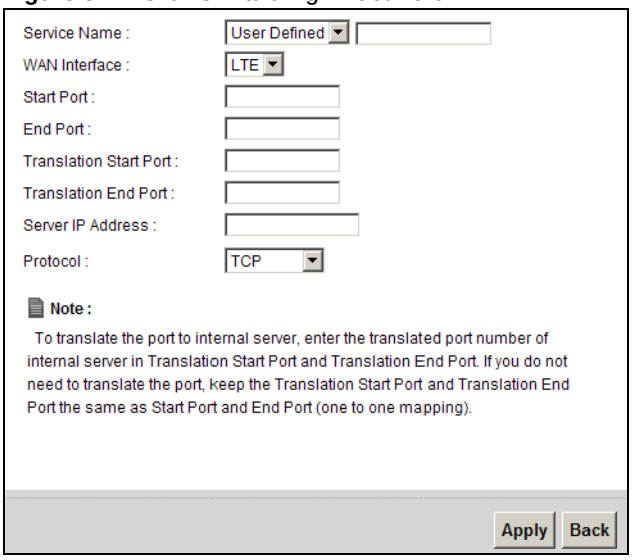
Table 21 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add new rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This is the service's name. This shows **User Defined** if you manually added a service. You can change this by clicking the edit icon.
WAN Interface	This shows the WAN interface through which the service is forwarded.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Server IP Address	This is the server's IP address.
Protocol	This shows the IP protocol supported by this virtual server, whether it is **TCP**, **UDP**, or **TCP/UDP**.
Modify	Click the **Edit** icon to edit the port forwarding rule. Click the **Delete** icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

8.2.2 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Click **Add new rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule to open the following screen.

Figure 32 Port Forwarding: Add/Edit


Service Name :
User Defined
WAN Interface :
LTE
Start Port :
End Port :
Translation Start Port :
Translation End Port :
Server IP Address :
Protocol :
TCP
Note :
To translate the port to internal server, enter the translated port number of internal server in Translation Start Port and Translation End Port. If you do not need to translate the port, keep the Translation Start Port and Translation End Port the same as Start Port and End Port (one to one mapping).
Apply
Back

The following table describes the labels in this screen.

Table 22 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	This is the WAN interface through which the service is forwarded.
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.
End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above.
Translation Start Port	This shows the port number to which you want the LTE Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

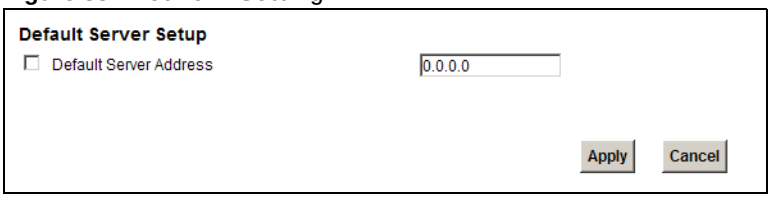
8.3 The DMZ Screen

Use this page to set the IP address of your network DMZ (if you have one) for the LTE Device. All incoming packets received by this LTE Device's WAN interface will be forwarded to the default server you set.

Click **Network Setting > NAT > DMZ** to display the following screen.

Note: The configuration you set in this screen takes priority than the **Network Setting > NAT > Port Forwarding** screen.

Figure 33 Network Setting > NAT > DMZ



The following table describes the fields in this screen.

Table 23 Network Setting > NAT > DMZ

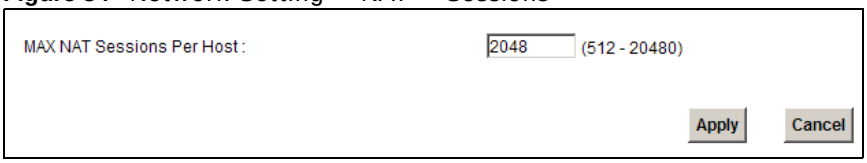
LABEL	DESCRIPTION
Default Server Address	Enter the IP address of your network DMZ host, if you have one. **0.0.0.0** means this feature is disabled.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

8.4 The Sessions Screen

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use.

Click **Network Setting > NAT > Sessions** to display the following screen.

Figure 34 Network Setting > NAT > Sessions



The following table describes the fields in this screen.

Table 24 Network Setting > NAT > Sessions

LABEL	DESCRIPTION
MAX NAT Session	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

8.5 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

8.5.1 NAT Definitions

Inside/outside denotes where a host is located relative to the LTE Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 25 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

8.5.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside

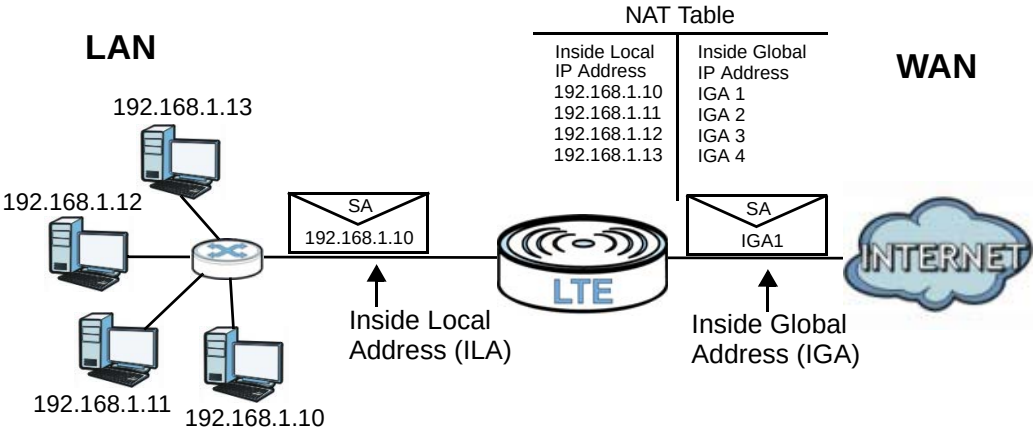
global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a Telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your LTE Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

8.5.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The LTE Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 35 How NAT Works



9

Dynamic DNS

9.1 Overview

This chapter discusses how to configure your LTE Device to use Dynamic DNS.

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in applications such as NetMeeting and CU-SeeMe). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

9.1.1 What You Need To Know

DYNDNS Wildcard

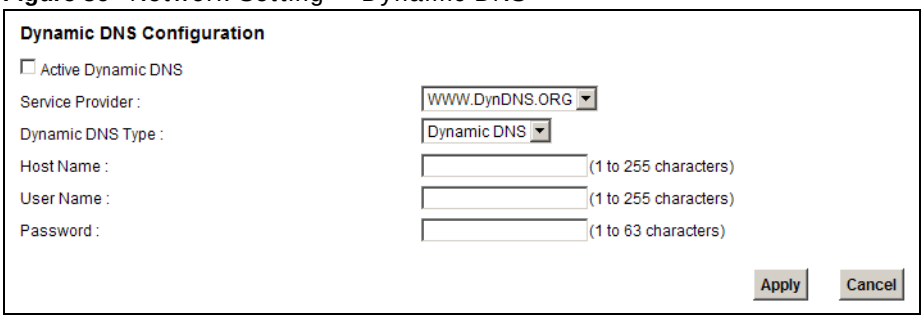
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

9.2 The Dynamic DNS Screen

Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the LTE Device. To change your LTE Device's DDNS, click **Network Setting > Dynamic DNS**. The screen appears as shown.

Figure 36 Network Setting > Dynamic DNS



The following table describes the fields in this screen.

Table 26 Network Setting > DNS

LABEL	DESCRIPTION
Dynamic DNS Configuration	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your LTE Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10

Firewall

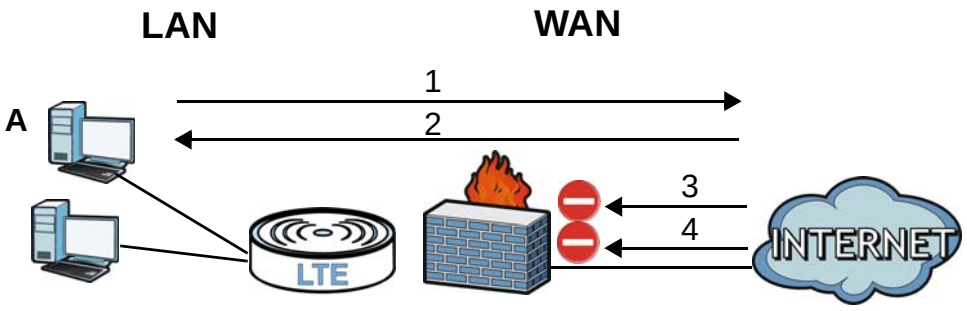
10.1 Overview

Use the LTE Device firewall screens to enable and configure the firewall that protects your LTE Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- Allows traffic that originates from your LAN computers to go to all other networks.
- Blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (**1**). Return traffic for this session is also allowed (**2**). However other traffic initiated from the WAN is blocked (**3** and **4**).

Figure 37 Default Firewall Action



10.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable the LTE Device's firewall (Section 10.2 on page 71).
- Use the **Services** screen to view the configured firewall rules and add, edit or remove a firewall rule (Section 10.3 on page 72).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 10.4 on page 73).
- Use the **DoS** screen to enable or disable Denial of Service (DoS) protection (Section 10.4 on page 73).

10.1.2 What You Need to Know

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The LTE Device is pre-configured to automatically detect and thwart all known DoS attacks.

Firewall

The LTE Device's firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is designed to protect against Denial of Service (DoS) attacks when activated. The LTE Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The LTE Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The LTE Device is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The LTE Device has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

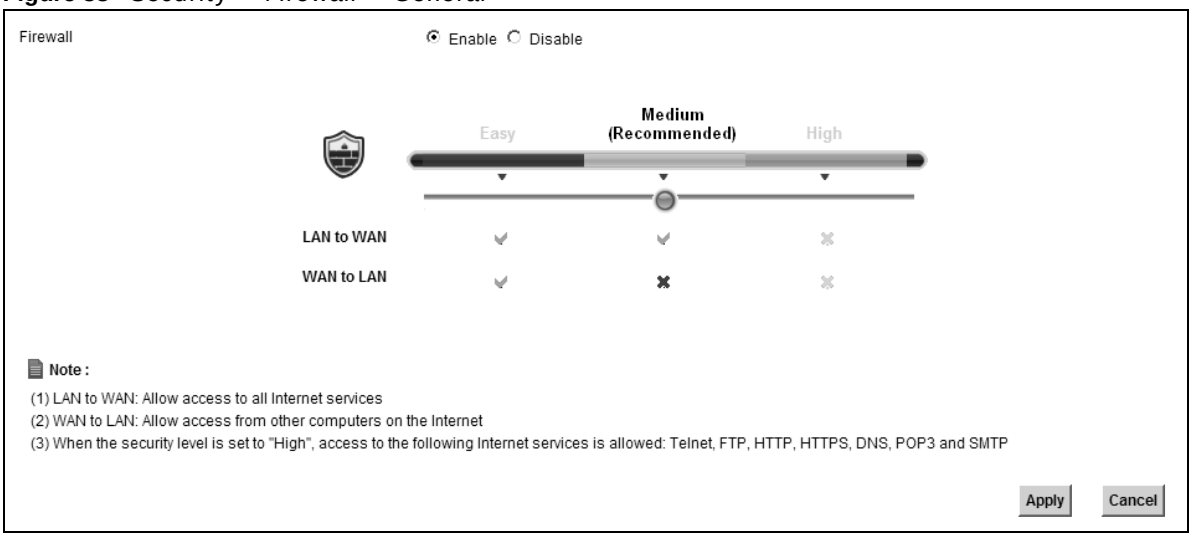
Finding Out More

See Section 10.6 on page 76 for advanced technical information on firewall.

10.2 The General Screen

Use this screen to enable or disable the LTE Device's firewall. Click **Security > Firewall** to open the **General** screen.

Figure 38 Security > Firewall > General


Firewall
Enable
Disable
Easy
Medium
(Recommended)
High
LAN to WAN
WAN to LAN
Note :
(1) LAN to WAN: Allow access to all Internet services
(2) WAN to LAN: Allow access from other computers on the Internet
(3) When the security level is set to "High", access to the following Internet services is allowed: Telnet, FTP, HTTP, HTTPS, DNS, POP3 and SMTP
Apply
Cancel

The following table describes the labels in this screen.

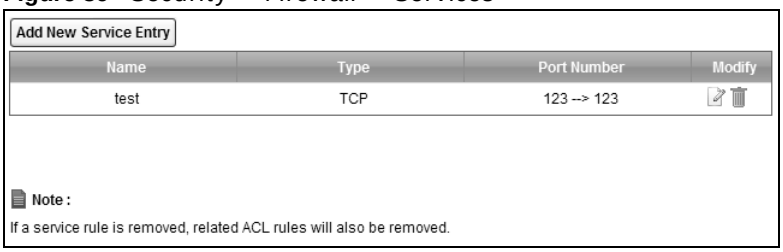
Table 27 Security > Firewall > General

LABEL	DESCRIPTION
Firewall	Select **Enable** to activate the firewall. The LTE Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Easy, Medium, High	Select **Easy** to have the firewall allow both LAN-to-WAN and WAN-to-LAN traffic to flow through the LTE Device. Select **Medium** to have the firewall only allow traffic sent from the LAN to the WAN. All traffic sent or access from the WAN will be blocked. Select **High** to have the firewall only allow Telnet, FTP, HTTP, HTTPS, DNS, POP3, and SMTP traffic sent from the LAN to the WAN. Other traffic will be blocked.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.3 The Services Screen

Use this screen to view the configured service list. To access this screen, click **Security > Firewall > Services**. You have to configure at least one service in this screen before configuring the **Security > Firewall > Access Control > Add New ACL Rule/Edit** screen.

Figure 39 Security > Firewall > Services



Each field is described in the following table.

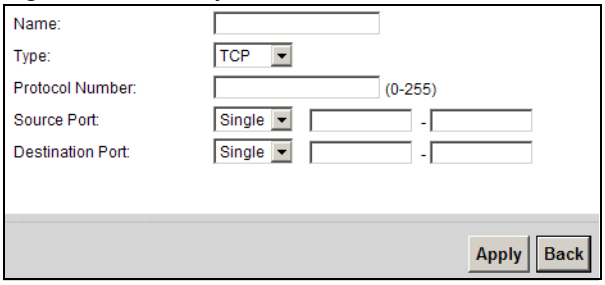
Table 28 Security > Firewall > Services

LABEL	DESCRIPTION
Add New Service Entry	Click this to define a new service.
Name	This is the name of a configured service.
Type	This is the protocol type (**TCP**, **UDP**, **ICMP** or **Others**) of the service.
Port Number	This displays a range of port numbers that defines the service.
Modify	Click the **Edit** icon to edit the service. Click the **Delete** icon to delete the service. Note that subsequent rules move up by one when you take this action. Deleting a service rule also deletes the related ACL rules which are configured in the **Security > Firewall > Access Control** screen.

10.3.1 The Add New Services Entry Screen

Use this screen to configure a service that you want to use in an ACL rule in the **Security > Firewall > Access Control > Add New ACL Rule/Edit** screen. To access this screen, click **Security > Firewall > Services** and then the **Add New Service Entry** button.

Figure 40 Security > Firewall > Services > Add New Service Entry



Each field is described in the following table.

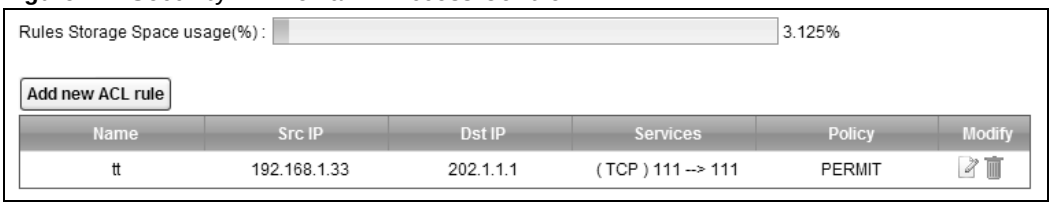
Table 29 Security > Firewall > Services > Add New Service Entry

LABEL	DESCRIPTION
Name	Type a descriptive name for the service.
Type	Select the protocol type (**TCP**, **UDP** or **ICMP or Others**) of the service.
Protocol Number	Enter the protocol number of the service type.
Source Port, Destination Port	The source port defines from which port number(s) the service traffic is sent. The destination port defines the port number(s) the destination hosts use to receive the service traffic. Select **Single** if the service uses one and only one source or destination port, then enter the port number. Select **Multiple** if the service uses two or more source or destination ports, then enter a port range. For example, suppose you want to define the Gnutella service. Select **TCP** type and enter a port range of **6345**-**6349**.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving your changes.

10.4 The Access Control Screen

Click **Security > Firewall > Access Control** to display the following screen. This screen displays a list of the configured incoming or outgoing filtering rules.

Figure 41 Security > Firewall > Access Control



Each field is described in the following table.

Table 30 Security > Firewall > Access Control

LABEL	DESCRIPTION
Rules Storage Space usage(%)	This bar shows the percentage of the LTE Device's space has been used. If the usage is almost full, you may need to remove an existing filter rule before you create a new one.
Add new ACL rule	Click this to go to add a filter rule for incoming or outgoing IP traffic.
Name	This displays the name of the rule.
Src IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to **Any**.
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to **Any**.
Services	This displays the protocol type and a port range that define the service to which this rule applies.

Table 30 Security > Firewall > Access Control (continued)

LABEL	DESCRIPTION
Policy	This field displays whether the rule silently discards packets (**DROP**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**REJECT**) or allows the passage of packets (**PERMIT**).
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.

10.4.1 The Add New ACL Rule/Edit Screen

Click **Add New ACL Rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays.

Figure 42 Security > Firewall > Access Control > Add New ACL Rule/Edit

Each field is described in the following table.

Table 31 Security > Firewall > Access Control > Add New ACL Rule/Edit

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule.
Source Address Type	Select **Single** or **Range** depending on whether you want to enter a single or a range of source IP address(es) to which the ACL rule applies. Select **Any** to indicate any source IP address.
Source IP Address Start	Enter an IP address or the starting IP address of the source IP range.
Source IP Address End	Enter the ending IP address of the source IP range.
Destination Address Type	Select **Single** or **Range** depending on whether you want to enter a single or a range of destination IP address(es) to which the ACL rule applies. Select **Any** to indicate any destination IP address.

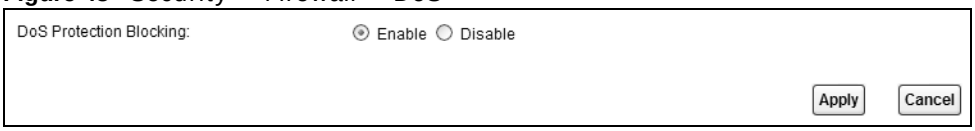
Table 31 Security > Firewall > Access Control > Add New ACL Rule/Edit (continued)

LABEL	DESCRIPTION
Destination IP Address Start	Enter an IP address or the starting IP address of the destination IP range.
Destination IP Address End	Enter the ending IP address of the destination IP range.
Select Protocol	Select the name of a configured service or select **Select Service** to define a new service in this screen.
Protocol	This field is available when you select **Select Service** in **Select Protocol**. Choose the protocol type (**TCP**, **UDP**, **ICMP** or **Others**) of the service.
Protocol Number	This field is available when you select **Others** in **Protocol**. Enter the protocol number of the service type to which this ACL rule applies.
Source Port	This field is displayed only when you select **Select Service** in **Select Protocol** and **TCP** or **UDP** in **Protocol**. Select **Single** or **Range** and then enter a single port number or the range of port numbers of the source. Select **Any** to indicate any source port.
Destination Port	This field is displayed only when you select **Select Service** in **Select Protocol** and **TCP** or **UDP** in **Protocol**. Select **Single** or **Range** and then enter a single port number or the range of port numbers of the destination. Select **Any** to indicate any destination port.
Policy	Use the drop-down list box to select whether to silently discard (**DROP**), deny and send an ICMP destination-unreachable message to the sender of (**REJECT**) or allow the passage of (**PERMIT**) packets that match this rule.
Direction	Use the drop-down list box to select the direction of traffic to which this rule applies. The possible options are **LAN to DEVICE**, **LAN to WAN**, **WAN to LAN**, and **WAN to DEVICE**.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving your changes.

10.5 The DoS Screen

Click **Security > Firewall > DoS** to display the following screen. Use this screen to enable or disable Denial of Service (DoS) protection.

Figure 43 Security > Firewall > DoS



Each field is described in the following table.

Table 32 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. Select **Enable** to enable protection against DoS attacks or **Disable** to disable it.
Apply	Click **Apply** to save the DoS Protection settings.
Cancel	Click **Cancel** to restore your previously saved settings.

10.6 Firewall Technical Reference

This section provides some technical background information about the topics covered in this chapter.

10.6.1 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your LTE Device.
4. Don't enable any local service (such as Telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Keep the firewall in a secured (locked) room.

10.6.2 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the LTE Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.

4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

11

MAC Filter

11.1 Overview

This chapter discusses MAC address filtering.

You can configure the LTE Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections.

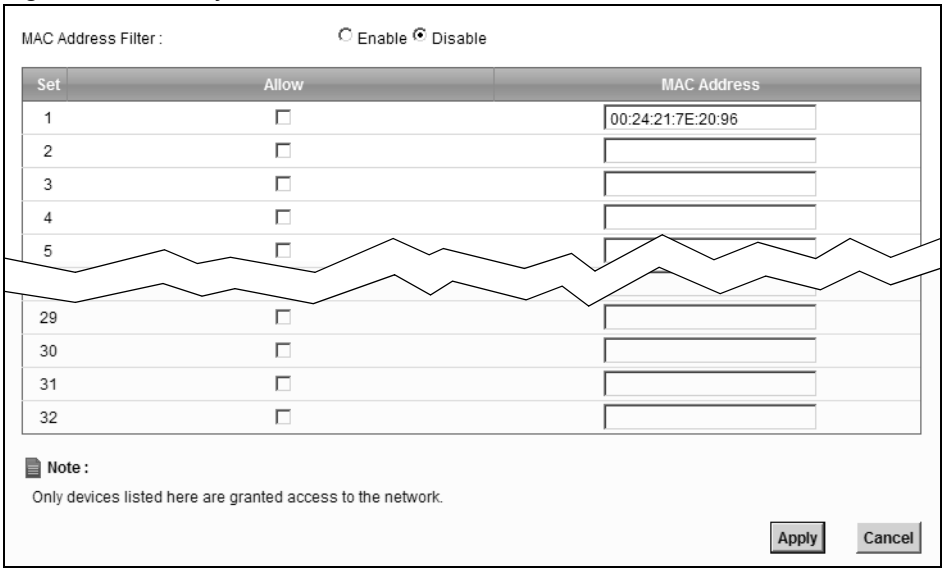
11.1.1 What You Need to Know

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

11.2 The MAC Filter Screen

Use the **MAC Filter** screen to allow wireless and LAN clients access to the LTE Device. To change your LTE Device's MAC filter settings, click **Security** > **MAC Filter**. The screen appears as shown.

Figure 44 Security > MAC Filter



The following table describes the labels in this menu.

Table 33 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select **Enable** to activate MAC address filtering.
Set	This is the index number of the MAC address.
Allow	Select **Allow** to permit access to the LTE Device. MAC addresses not listed will be denied access to the LTE Device. If you clear this, the **MAC Address** field for this set clears.
MAC Address	Enter the MAC addresses of the wireless station and LAN devices that are allowed access to the LTE Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

12

Parental Control

12.1 Overview

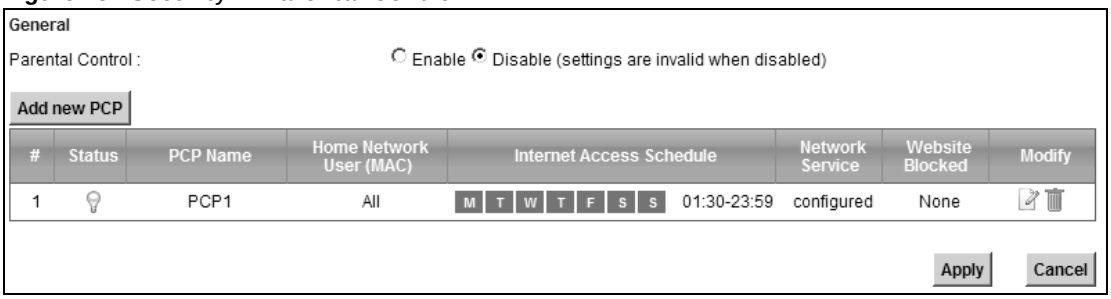
Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the LTE Device performs parental control on a specific user.

12.2 The Parental Control Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Security > Parental Control** to open the following screen.

Figure 45 Security > Parental Control



The following table describes the fields in this screen.

Table 34 Parental Control > Parental Control

LABEL	DESCRIPTION
Parental Control	Select **Enable** to activate parental control.
Add new PCP	Click this if you want to configure a new parental control rule.
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User (MAC)	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, **None** will be shown.

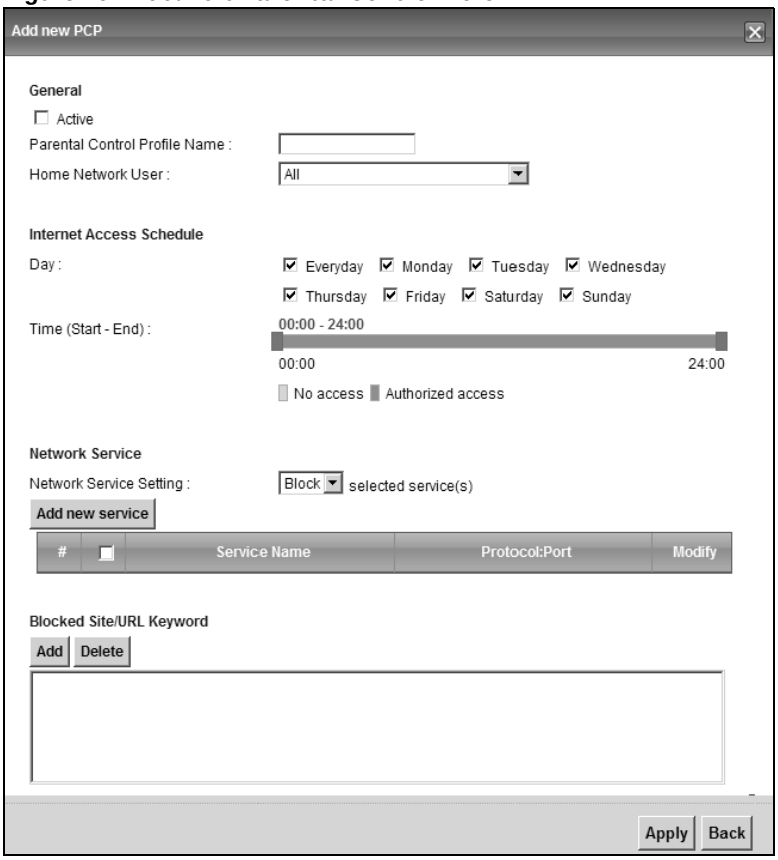
Table 34 Parental Control > Parental Control (continued)

LABEL	DESCRIPTION
Website Block	This shows whether the website block is configured. If not, **None** will be shown.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Add	Click **Add** to create a new schedule.
Apply	Click **Apply** to save your changes back to the LTE Device.

12.2.1 Add/Edit a Parental Control Rule

Click **Add new PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 46 Add/Edit Parental Control Rule



The following table describes the fields in this screen.

Table 35 Add/Edit Parental Control Rule

LABEL	DESCRIPTION
General	
Active	Select the checkbox to activate this parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.

Table 35 Add/Edit Parental Control Rule (continued)

LABEL	DESCRIPTION
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select **Custom**, enter the LAN user's MAC address. If you select **All**, the rule applies to all LAN users.
Internet Access Schedule	
Day	Select check boxes for the days that you want the LTE Device to perform parental control.
Start Blocking Time End Blocking Time	Enter the time period of each day, in 24-hour format, during which parental control will be enforced.
Time	Drag the time bar to define the time that the LAN user is allowed access.
Network Service	
Network Service Setting	If you select **Block**, the LTE Device prohibits the users from viewing the Web sites with the URLs listed below. If you select **Access**, the LTE Device blocks access to all URLs except ones listed below.
Add new service	Click this to show a screen in which you can add a new service rule. You can configure the **Service Name**, **Protocol**, and **Port** of the new rule.
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Blocked Site/URL Keyword	Click **Add** to show a screen to enter the URL of web site or URL keyword to which the LTE Device blocks access. Click **Delete** to remove it.
Apply	Click this button to save your settings back to the LTE Device.
Back	Click this button to return to the previous screen without saving any changes.

13.1 Overview

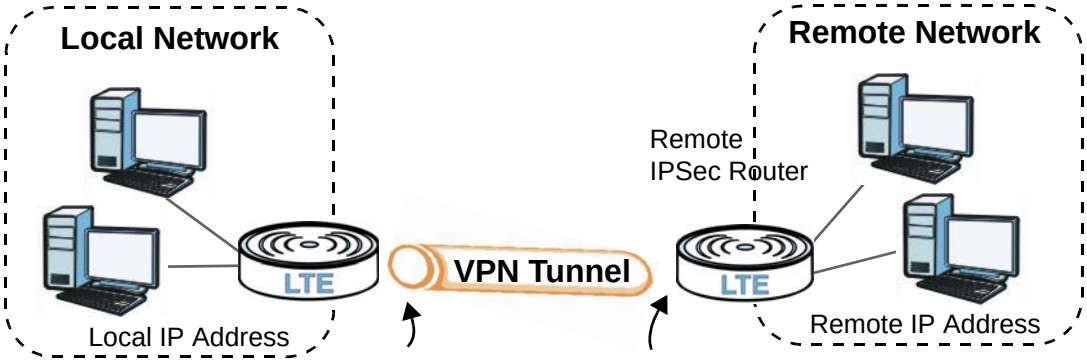
This chapter shows you how to configure the LTE Device's VPN settings.

13.2 IPSec VPN

13.2.1 The General Screen

The following figure helps explain the main fields in the web configurator.

Figure 47 IPSec Fields Summary



Click **Security > VPN** to open this screen as shown next.

Figure 48 IPSec VPN

This screen contains the following fields:

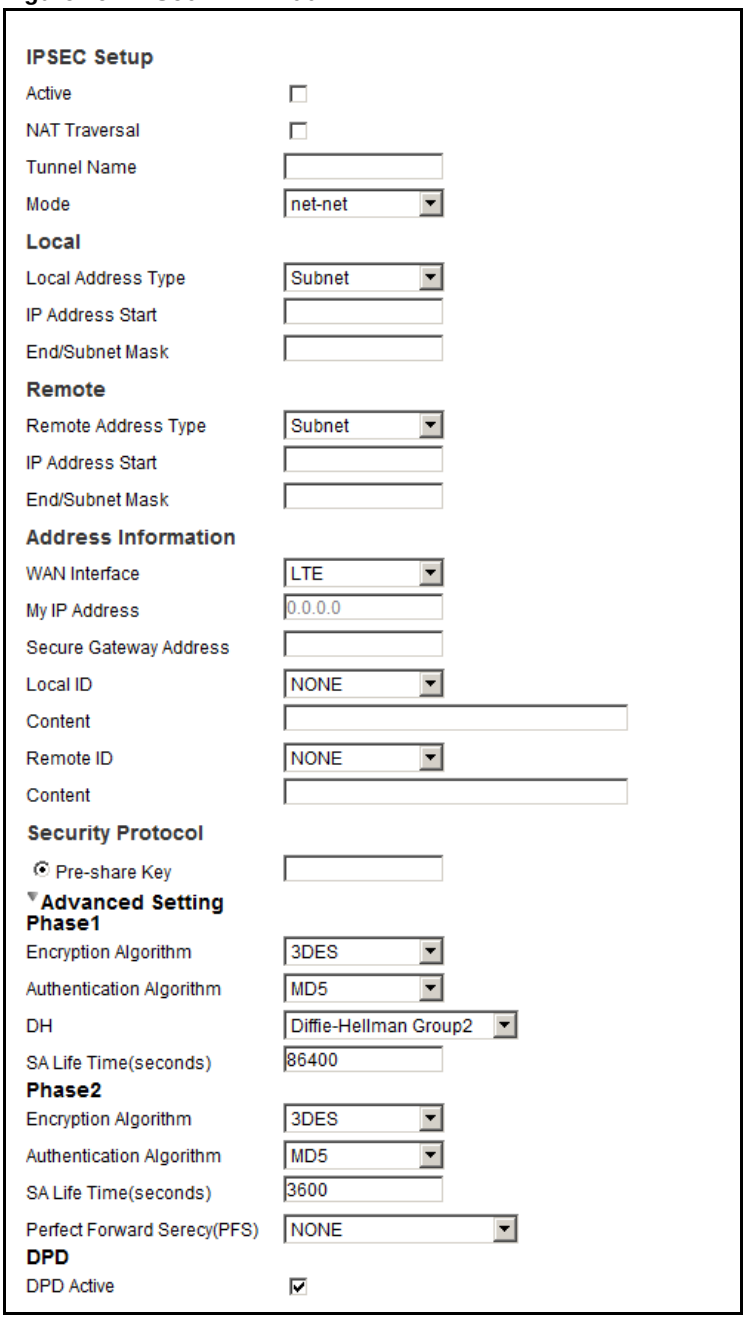
Table 36 IPSec VPN

LABEL	DESCRIPTION
Add New Tunnel	Click this button to add an item to the list.
#	This is the VPN policy index number.
Active	This displays if the VPN policy is enabled.
Tunnel Name	Enter the name of the VPN connection.
Local Address	This displays the IP address of the LTE Device.
Remote Address	This displays the IP address of the remote IPSec router.
IPSec Algorithm	This displays the encryption algorithm being used for the VPN connection.

13.2.2 IPSec VPN: Add

Use these settings. Click **Security > VPN > Add New Tunnel** to open this screen as shown next.

Figure 49 IPSec VPN: Add



This screen contains the following fields:

Table 37 IPSec VPN: Add

LABEL	DESCRIPTION
IPSEC Setup	
Active	Select **Active** to activate this VPN policy.

Table 37 IPSec VPN: Add

LABEL	DESCRIPTION
NAT Traversal	Select this if any of these conditions are satisfied. • This IKE SA might be used to negotiate IPSec SAs that use ESP as the active protocol. • There are one or more NAT routers between the LTE Device and remote IPSec router, and these routers do not support IPSec pass-thru or a similar feature. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged.
Tunnel Name	Enter the name of the VPN connection.
Mode	Select the encapsulation mode. When **net-net** is selected, the connection will operate in tunnel mode.
Local	
Local Address Type	Select **Single** or **Subnet** to specify if the VPN connection begins at an IP address or subnet.
IP Address Start	If **Single** is selected, enter a (static) IP address on the LAN behind your LTE Device. If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind your LTE Device. Then enter the subnet mask to identify the network address.
End/Subnet Mask	If **Subnet** is selected, enter the subnet mask to identify the network address.
Remote	
Remote Address Type	Select **Single** or **Subnet** to specify if the VPN connection terminates at an IP address or subnet.
IP Address Start	If **Single** is selected, enter a (static) IP address on the LAN behind the remote IPSec's router. If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind the remote IPSec's router. Then enter the subnet mask to identify the network address.
End/Subnet Mask	If **Subnet** is selected, enter the subnet mask to identify the network address.
Address Information	
WAN Interface	Select the interface for the VPN gateway.
My IP Address	Enter the IP address of the LTE Device in the IKE SA.
Secure Gateway Address	Enter the IP address of the remote IPSec router in the IKE SA.
Local ID	Select **IP** to identify the LTE Device by its IP address. Select **DNS** to identify this LTE Device by a domain name. Select **E-mail** to identify this LTE Device by an e-mail address.

Table 37 IPSec VPN: Add

LABEL	DESCRIPTION
Content	When you select **IP** in the **Local ID** field, type the IP address of your computer in the **Content** field. If you configure the **Content** field to 0.0.0.0 or leave it blank, the LTE Device automatically uses the **Pre-Share Key** (refer to the **Pre-Share Key** field description). It is recommended that you type an IP address other than 0.0.0.0 in the **Content** field or use the **DNS** or **E-mail** ID type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID** field, type a domain name or e-mail address by which to identify this LTE Device in the **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Remote ID	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	The configuration of the remote content depends on the remote ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to 0.0.0.0 or leave it blank, the LTE Device will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than 0.0.0.0 or use the **DNS** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the LTE Device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
Security Protocol	
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself.
Advanced Setting - Phase 1	

Table 37 IPSec VPN: Add

LABEL	DESCRIPTION
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The LTE Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **MD5**, **SHA1**, **SHA2-256** and **SHA2-512**. **SHA** is generally considered stronger than **MD5**, but it is also slower.
DH	Select which Diffie-Hellman key group you want to use for encryption keys. Choices are: **Diffie-Hellman Group2** - use a 1024-bit random number **Diffie-Hellman Group5** - use a 1536-bit random number **Diffie-Hellman Group14** - use a 2048-bit random number The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
SA Life Time	Define the length of time before an IPSec SA automatically renegotiates in this field. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Phase 2	
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The LTE Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **MD5**, **SHA1**, **SHA2-256** and **SHA2-512**. **SHA** is generally considered stronger than **MD5**, but it is also slower.

Table 37 IPSec VPN: Add

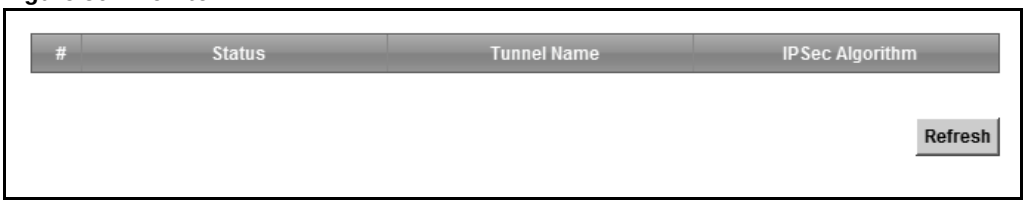
LABEL	DESCRIPTION
SA Life Time	Define the length of time before an IPSec SA automatically renegotiates in this field. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. Choices are: **Diffie-Hellman Group2** - use a 1024-bit random number **Diffie-Hellman Group5** - use a 1536-bit random number **Diffie-Hellman Group14** - use a 2048-bit random number
DPD Active	Select the Dead Peer Detection (DPD) Active check box if you want the LTE Device to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If the remote IPSec router does not respond, the LTE Device shuts down the IKE SA. If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check.

13.2.3 The Monitor Screen

The following figure helps explain the main fields in the web configurator.

Click **Security > VPN > Monitor** to open this screen as shown next.

Figure 50 Monitor



This screen contains the following fields:

Table 38 Monitor

LABEL	DESCRIPTION
#	This is the VPN policy index number.
Status	This displays if the VPN policy is connected.
Tunnel Name	Enter the name of the VPN connection.
IPSec Algorithm	This displays the encryption algorithm being used for the VPN connection.
Refresh	Click this button to refresh the information on the screen.

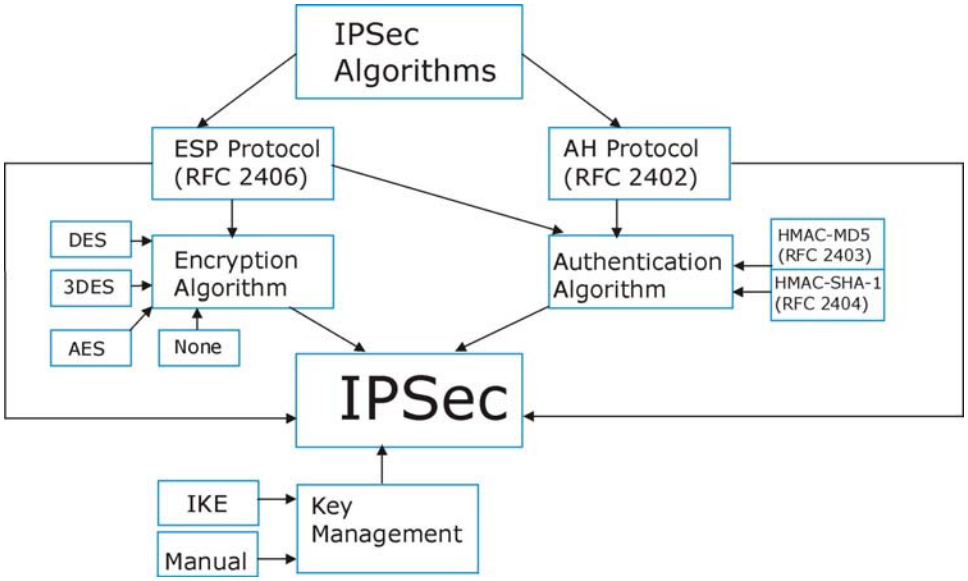
13.3 Technical Reference

This section provides some technical background information about the topics covered in this section.

13.3.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 51 IPSec Architecture



IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

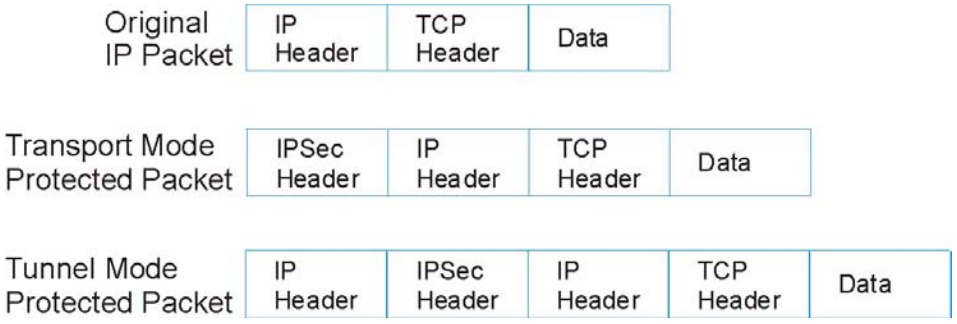
Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

13.3.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the LTE Device supports **Tunnel** mode only.

Figure 52 Transport and Tunnel Mode IPSec Encapsulation



Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

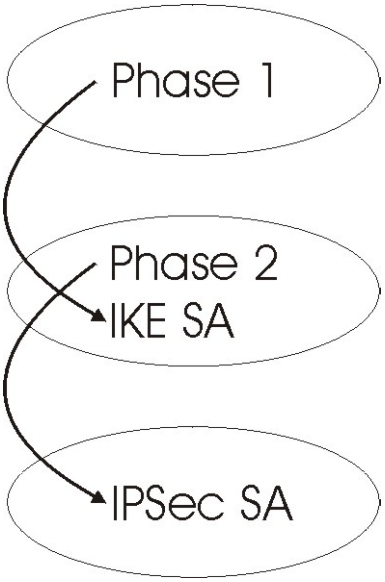
Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

13.3.3 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 53 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The LTE Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

13.3.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

13.3.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the LTE Device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 39 VPN and NAT

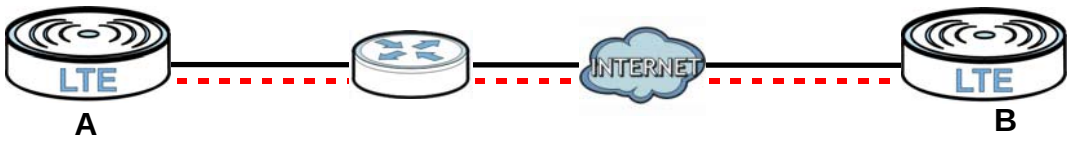
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

13.3.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the LTE Device's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 54 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In the above figure, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 40 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the LTE Device if you enable NAT traversal.

13.3.7 ID Type and Content

With aggressive negotiation mode (see Section 13.3.4 on page 94), the LTE Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the LTE Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the LTE Device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 13.3.4 on page 94), the ID type and content are encrypted to provide identity protection. In this case the LTE Device can distinguish between different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The LTE Device can

distinguish different incoming SAs and you can select between different encryption algorithms, authentication algorithms and key groups when you configure a VPN rule. The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 41 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer.
DNS	Type a domain name (up to 31 characters) by which to identify this LTE Device.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this LTE Device.
	The domain name or e-mail address that you use in the **Local ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

13.3.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two LTE Devices in this example can complete negotiation and establish a VPN tunnel.

Table 42 Matching ID Type and Content Configuration Example

LTE Device A	LTE Device B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Remote ID type: IP	Remote ID type: E-mail
Remote ID content: 1.1.1.2	Remote ID content: tom@yourcompany.com

The two LTE Devices in this example cannot complete their negotiation because LTE Device B's **Local ID type** is **IP**, but LTE Device A's **Remote ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 43 Mismatching ID Type and Content Configuration Example

LTE DEVICE A	LTE DEVICE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.2
Remote ID type: E-mail	Remote ID type: IP
Remote ID content: aa@yahoo.com	Remote ID content: 1.1.1.0

13.3.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 13.3.3 on page 94 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

13.3.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

14 Logs

14.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the LTE Device log and then display the logs or have the LTE Device send them to an administrator (as e-mail) or to a syslog server.

14.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs for the categories that you select (Section 14.2 on page 100).

14.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 44 Syslog Severity Levels

CODE	SEVERITY
0	Emergency (EMERG): The system is unusable.
1	Alert (ALERT): Action must be taken immediately.
2	Critical (CRIT): The system condition is critical.
3	Error (ERROR): There is an error condition on the system.
4	Warning (WARNING): There is a warning condition on the system.
5	Notice (NOTICE): There is a normal but significant condition on the system.

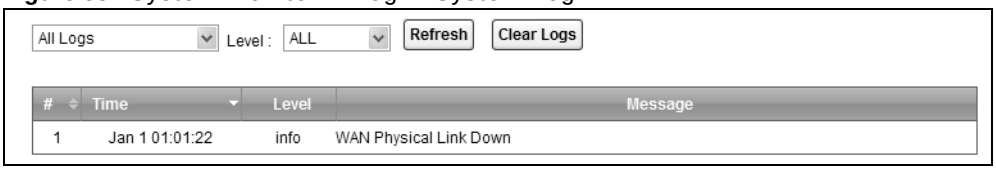
Table 44 Syslog Severity Levels (continued)

CODE	SEVERITY
6	Informational (INFO): The syslog contains an informational message.
7	Debug (DEBUG): The message is intended for debug-level purposes.

14.2 The System Log Screen

Click **System Monitor > Log** to open the **System Log** screen. Use the **System Log** screen to see the system logs for the categories that you select in the upper left drop-down list box.

Figure 55 System Monitor > Log > System Log



The following table describes the fields in this screen.

Table 45 System Monitor > Log > System Log

LABEL	DESCRIPTION
	Select the type of the logs that you want to search in the first drop-down list box.
Level	Select a severity level from this drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the LTE Device searches through all logs of that severity or higher. See Table 44 on page 99 for more information about severity levels.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the date and time the log was recorded.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Message	This field states the reason for the log.

15

Traffic Status

15.1 Overview

Use the **Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT.

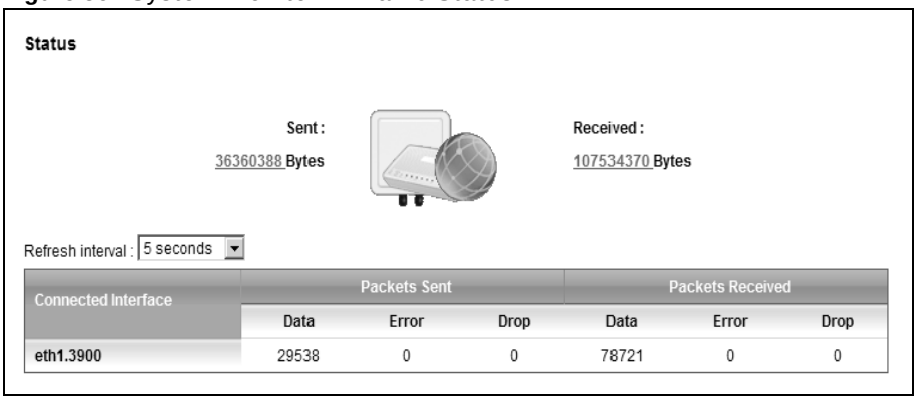
15.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 15.2 on page 101).
- Use the **LAN** screen to view the LAN traffic statistics (Section 15.3 on page 102).
- Use the **NAT** screen to view the NAT status of the LTE Device's client(s) (Section 15.4 on page 103).

15.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. You can view the WAN traffic statistics in this screen.

Figure 56 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 46 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Status	This shows the number of bytes received and sent through the WAN interface of the LTE Device.
Refresh Interval	Select how often you want the LTE Device to update this screen from the drop-down list box.

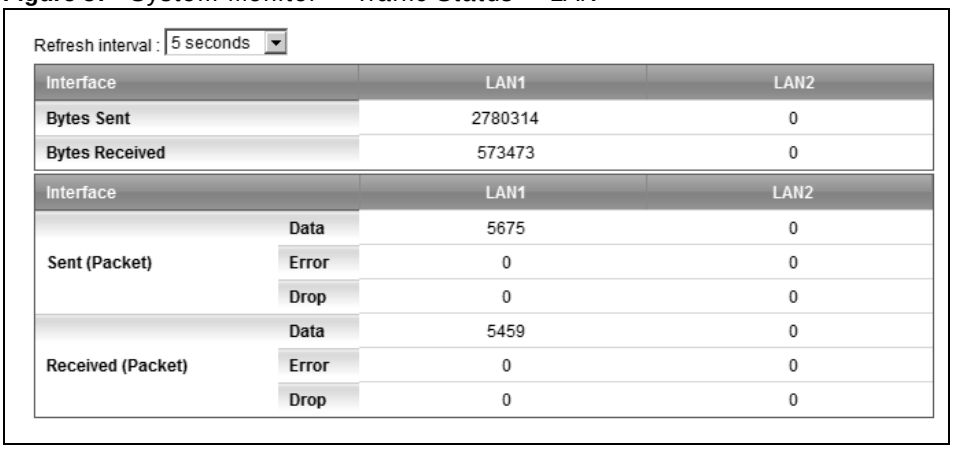
Table 46 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

15.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. You can view the LAN traffic statistics in this screen.

Figure 57 System Monitor > Traffic Status > LAN



The following table describes the fields in this screen.

Table 47 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the LTE Device to update this screen from the drop-down list box.
Interface	This shows the LAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN interface.
Sent (Packet)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.

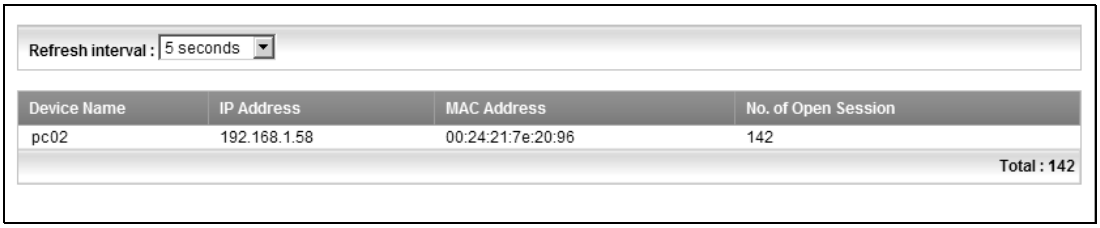
Table 47 System Monitor > Traffic Status > LAN (continued)

LABEL	DESCRIPTION
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packet)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

15.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. You can view the NAT status of the LTE Device's client(s) in this screen.

Figure 58 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

Table 48 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the LTE Device to update this screen from the drop-down list box.
Device Name	This shows the name of the client.
IP Address	This shows the IP address of the client.
MAC Address	This shows the MAC address of the client.
No. of Open Session	This shows the number of NAT sessions used by the client.

16

User Account

16.1 Overview

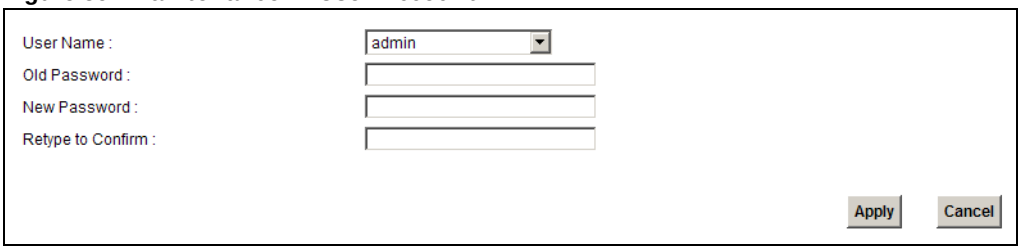
You can configure system password for different user accounts in the **User Account** screen.

16.2 The User Account Screen

Use the **User Account** screen to configure system password.

Click **Maintenance > User Account** to open the following screen.

Figure 59 Maintenance > User Account



The following table describes the labels in this screen.

Table 49 Maintenance > User Account

LABEL	DESCRIPTION
User Name	You can configure the password for the **Power User** and **Admin** accounts.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the LTE Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

17

Remote MGMT

17.1 Overview

Remote MGMT allows you to manage your LTE Device from a remote location through the following interfaces:

- LAN
- WAN only

Note: The LTE Device is managed using the web configurator.

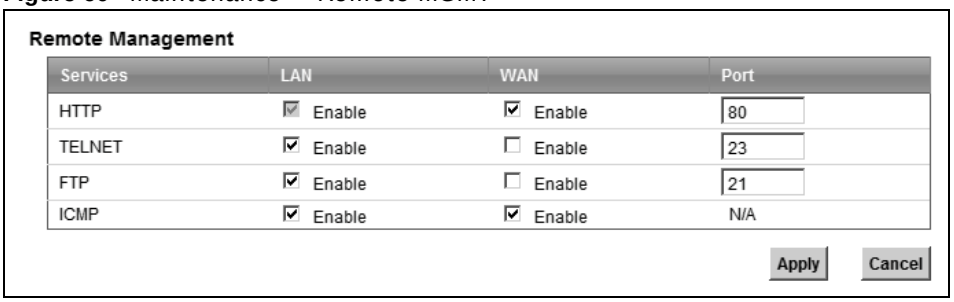
17.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter

17.2 The Remote MGMT Screen

Use this screen to decide what services you may use to access which LTE Device interface. Click **Maintenance > Remote MGMT** to open the following screen.

Figure 60 Maintenance > Remote MGMT



The following table describes the fields in this screen.

Table 50 Maintenance > Remote MGMT

LABEL	DESCRIPTION
Services	This is the service you may use to access the LTE Device.
LAN	Select the **Enable** check box for the corresponding services that you want to allow access to the LTE Device from the LAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the LTE Device from the WAN.

Table 50 Maintenance > Remote MGMT (continued)

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

18

System

18.1 Overview

You can configure system settings, including the host name, domain name and the inactivity time-out interval in the **System** screen.

18.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter.

Domain Name

This is a network address that identifies the owner of a network connection. For example, in the network address “www.example.com/support/files”, the domain name is “www.example.com”.

18.2 The System Screen

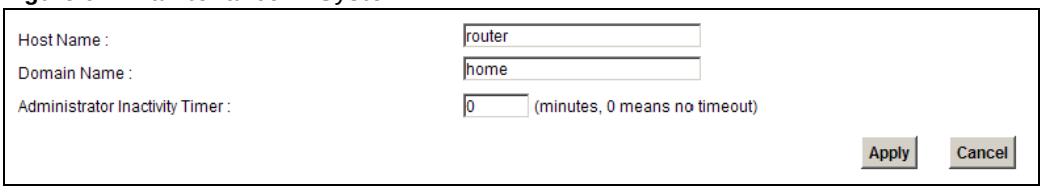
Use the **System** screen to configure the system’s host name, domain name, and inactivity time-out interval.

The **Host Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer.

In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the LTE Device **System Name**.

Click **Maintenance > System** to open the following screen.

Figure 61 Maintenance > System



The following table describes the labels in this screen.

Table 51 Maintenance > System

LABEL	DESCRIPTION
Host Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click this to save your changes back to the LTE Device.
Cancel	Click this to begin configuring this screen afresh.

19

Time Setting

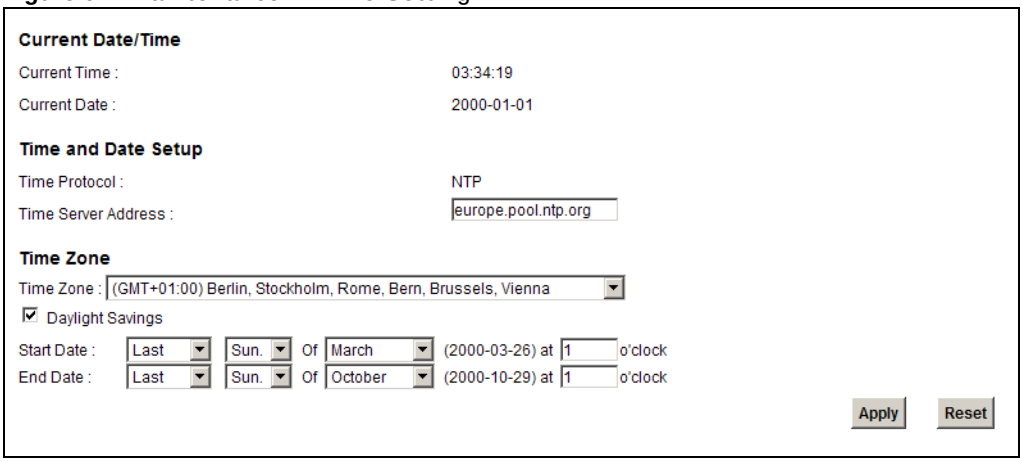
19.1 Overview

You can configure the system's time and date in the **Time Setting** screen.

19.2 The Time Setting Screen

To change your LTE Device's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the LTE Device's time based on your local time zone.

Figure 62 Maintenance > Time Setting



The following table describes the fields in this screen.

Table 52 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your LTE Device.
Current Date	This field displays the date of your LTE Device.
Time and Date Setup	
Time Protocol	This shows the time service protocol that your time server sends when you turn on the LTE Device.
Time Server Address	Enter the IP address or URL (up to 31 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Table 52 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type **2** in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type **2** in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

20

Log Setting

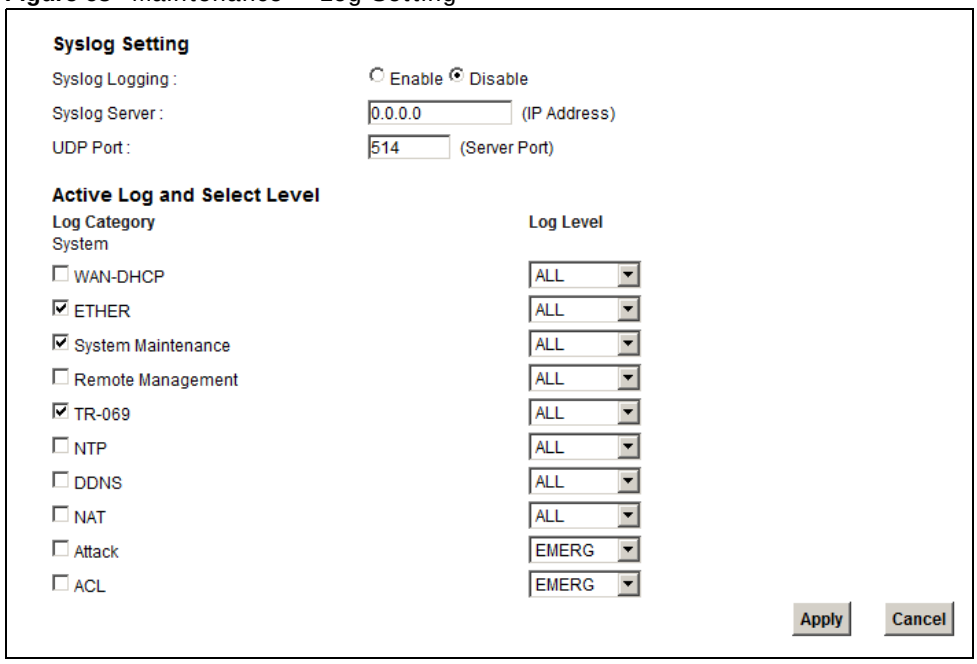
20.1 Overview

You can configure where the LTE Device sends logs and which logs and/or immediate alerts the LTE Device records in the **Log Setting** screen.

20.2 The Log Setting Screen

To change your LTE Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

Figure 63 Maintenance > Log Setting



The following table describes the fields in this screen.

Table 53 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The LTE Device sends a log to an external syslog server. Select the **Enable** check box to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.

Table 53 Maintenance > Log Setting (continued)

LABEL	DESCRIPTION
UDP Port	Enter the port number used by the syslog server.
Active Log and Select Level	
Log Category	Select the categories of logs that you want to record.
Log Level	Select the severity level of logs that you want to record. If you want to record all logs, select **ALL**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

21

Firmware Upgrade

21.1 Overview

This chapter explains how to upload new firmware to your LTE Device. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

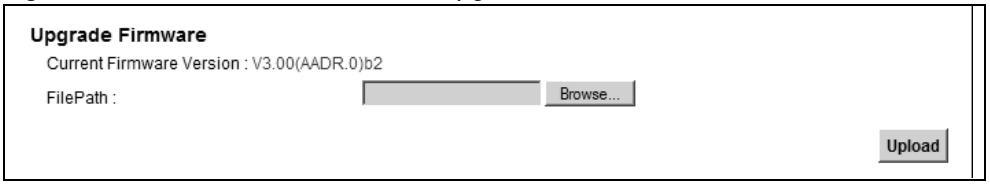
Only use firmware for your device's specific model. Refer to the label on the bottom of your LTE Device.

21.2 The Firmware Upgrade Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three minutes. After a successful upload, the system will reboot.

Do NOT turn off the LTE Device while firmware upload is in progress!

Figure 64 Maintenance > Firmware Upgrade



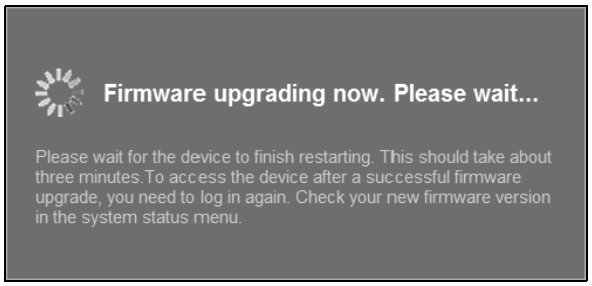
The following table describes the labels in this screen.

Table 54 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to three minutes.

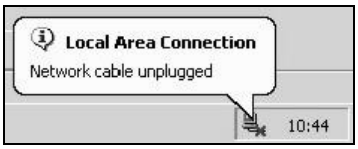
After you see the firmware updating screen, wait a few minutes before logging into the LTE Device again.

Figure 65 Firmware Uploading


Firmware upgrading now. Please wait...
Please wait for the device to finish restarting. This should take about three minutes.To access the device after a successful firmware upgrade, you need to log in again. Check your new firmware version in the system status menu.

The LTE Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

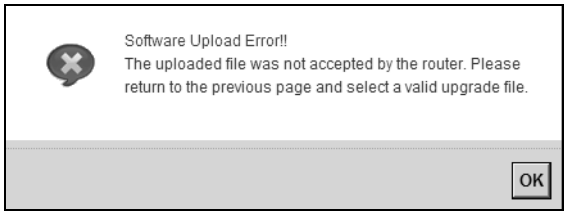
Figure 66 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 67 Error Message


Software Upload Error!!
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file.
OK

22

Backup/Restore

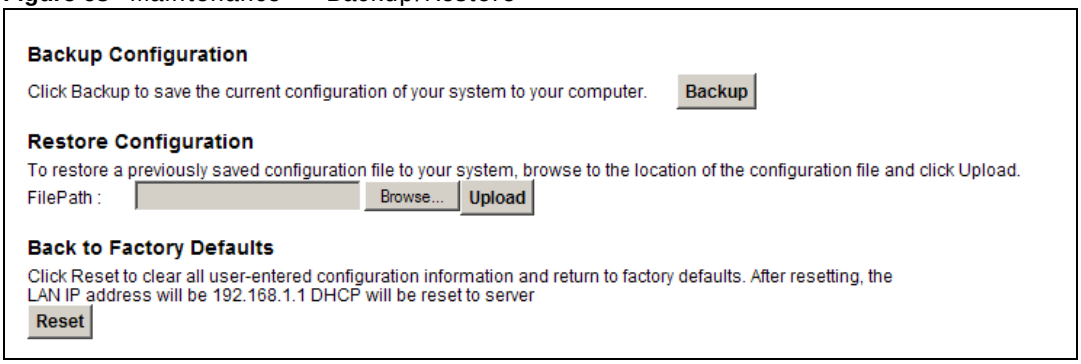
22.1 Overview

The **Backup / Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

22.2 The Backup/Restore Screen

Click **Maintenance > Backup / Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 68 Maintenance > Backup/Restore


Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
FilePath :
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the LAN IP address will be 192.168.1.1 DHCP will be reset to server
Reset

Backup Configuration

Backup Configuration allows you to back up (save) the LTE Device's current configuration to a file on your computer. Once your LTE Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the LTE Device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your LTE Device.

Table 55 Restore Configuration

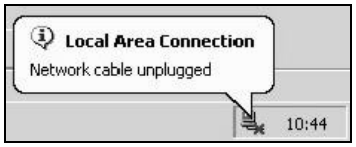
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your device settings back to the factory default.

Do not turn off the LTE Device while configuration file upload is in progress.

After the LTE Device configuration has been restored successfully, the login screen appears. Login again to restart the LTE Device.

The LTE Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 69 Network Temporarily Disconnected



If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix B on page 137 for details on how to set up your computer's IP address.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the LTE Device to its factory defaults. The following warning screen appears.

Figure 70 Reset Warning Message

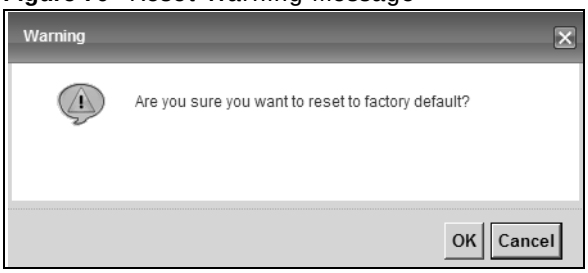
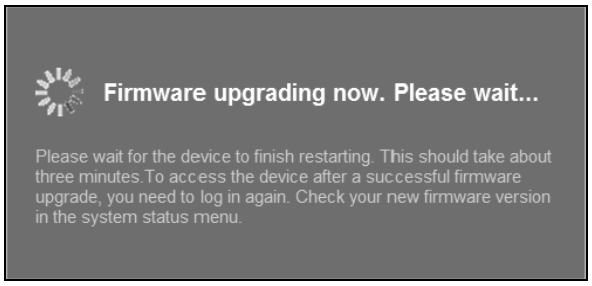


Figure 71 Reset In Process Message


Firmware upgrading now. Please wait...
Please wait for the device to finish restarting. This should take about three minutes.To access the device after a successful firmware upgrade, you need to log in again. Check your new firmware version in the system status menu.

You can also press the **RESET** button on the back panel to reset the factory defaults of your LTE Device. Refer to Section 1.6 on page 15 for more information on the **RESET** button.

22.3 The Reboot Screen

System restart allows you to reboot the LTE Device remotely without turning the power off. You may need to do this if the LTE Device hangs, for example.

Click **Maintenance > Reboot**. Click the **Reboot** button to have the LTE Device reboot. This does not affect the LTE Device's configuration.

23

Diagnostic

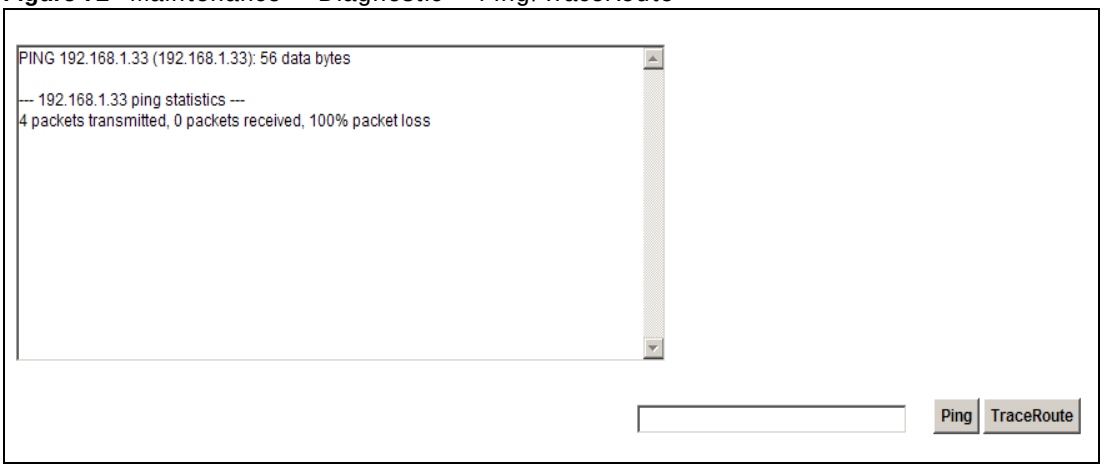
23.1 Overview

You can use different diagnostic methods to test a connection and see the detailed information. These read-only screens display information to help you identify problems with the LTE Device.

23.2 The Ping/TraceRoute Screen

Ping and traceroute help check availability of remote hosts and also help troubleshoot network or Internet connections. Click **Maintenance > Diagnostic** to open the **Ping / TraceRoute** screen shown next.

Figure 72 Maintenance > Diagnostic > Ping/TraceRoute


PING 192.168.1.33 (192.168.1.33): 56 data bytes
--- 192.168.1.33 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
Ping
TraceRoute

The following table describes the fields in this screen.

Table 56 Maintenance > Diagnostic > Ping/TraceRoute

LABEL	DESCRIPTION
Ping	Type the IP address of a computer that you want to ping in order to test a connection. Click **Ping** and the ping statistics will show in the diagnostic .
TraceRoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified host.

24

Troubleshooting

24.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- LTE Device Access and Login
- Internet Access
- UPnP

24.2 Power, Hardware Connections, and LEDs

The LTE Device does not turn on. None of the LEDs turn on.

1. Make sure the LTE Device is turned on.
2. Make sure you are using the power adaptor or cord included with the LTE Device.
3. Make sure the power adaptor or cord is connected to the LTE Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the LTE Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 14.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the LTE Device off and on.

5 If the problem continues, contact the vendor.

24.3 LTE Device Access and Login

I forgot the IP address for the LTE Device.

1 The default IP address is 192.168.1.1.

2 If you changed the IP address and have forgotten it, you might get the IP address of the LTE Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the LTE Device (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 15.

I forgot the password.

1 The default admin password is **1234** and the default user password is **1234**.

2 If you can't remember the password, you have to reset the device to its factory defaults. See Section 1.6 on page 15.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the LTE Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix C on page 167.

4 Reset the device to its factory defaults, and try to access the LTE Device with the default IP address. See Section 1.6 on page 15.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the LTE Device using another service, such as Telnet. If you can access the LTE Device, check the remote management settings and firewall rules to find out why the LTE Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the LTE Device.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the LTE Device. Log out of the LTE Device in the other session, or ask the person who is logged in to log out.

3 Turn the LTE Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 24.2 on page 123.

24.4 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 14.

2 Make sure you entered your service provider's LTE APN information correctly.

3 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

4 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the LTE Device), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 14.

2 Turn the LTE Device off and on.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 14. If the LTE Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Turn the LTE Device off and on.

3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

24.5 UPnP

When using UPnP and the LTE Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1 Disconnect the Ethernet cable from the LTE Device's LAN port or from your computer.

2 Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

1 Wait more than three minutes.

2 Restart the applications.

A

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (such as computers, servers, routers, and printers) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

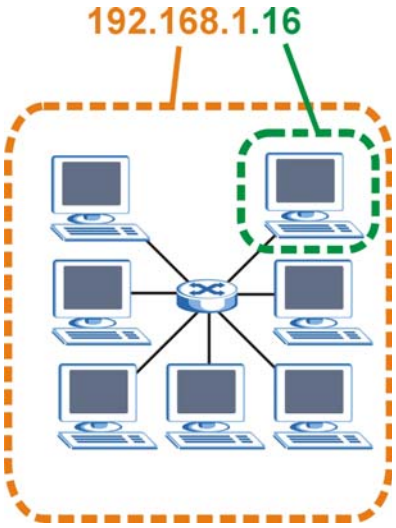
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 73 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 57 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 58 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 59 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 60 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

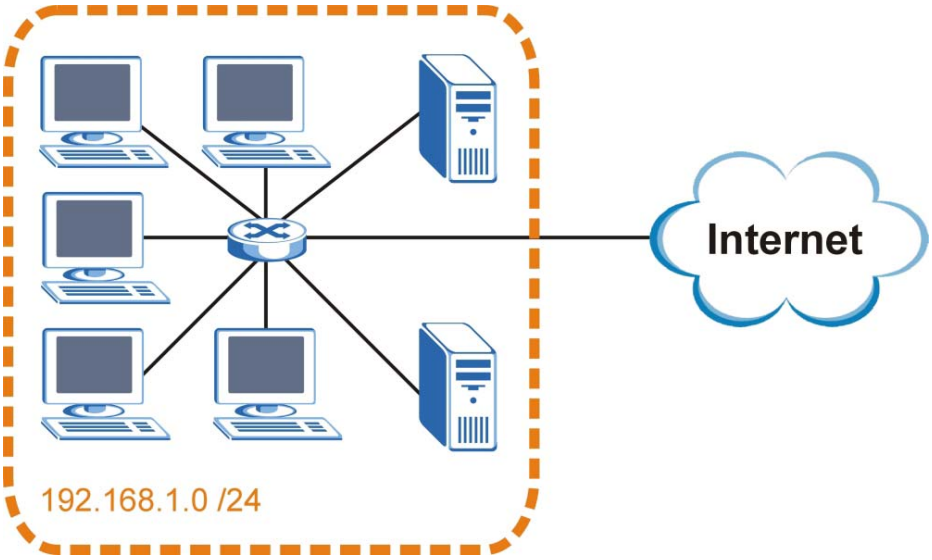
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 74 Subnetting Example: Before Subnetting

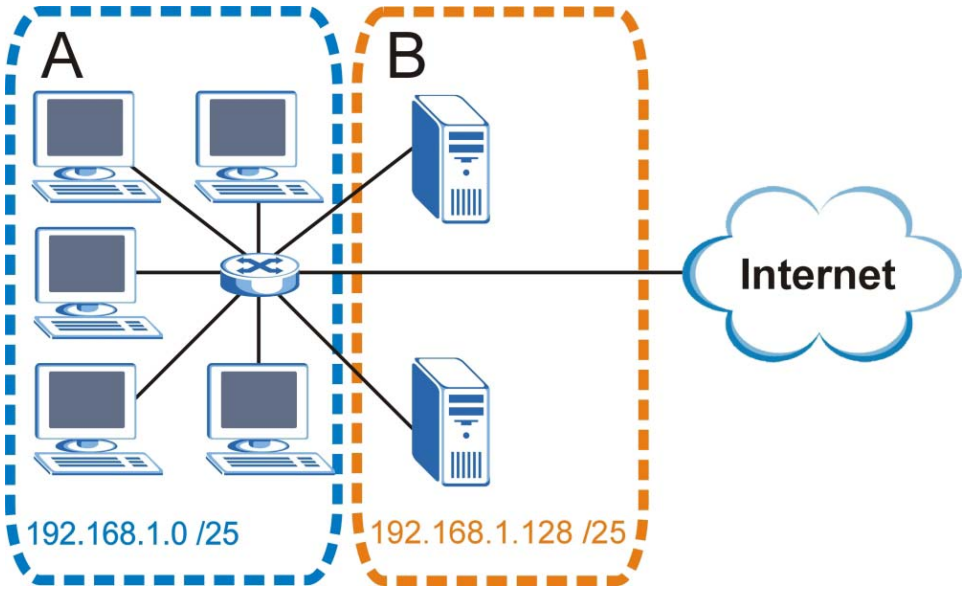


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 75 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 61 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000

Table 61 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 62 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 63 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 64 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 65 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 66 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 67 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14

Table 67 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the LTE Device.

Once you have decided on the network number, pick an IP address for your LTE Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your LTE Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the LTE Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

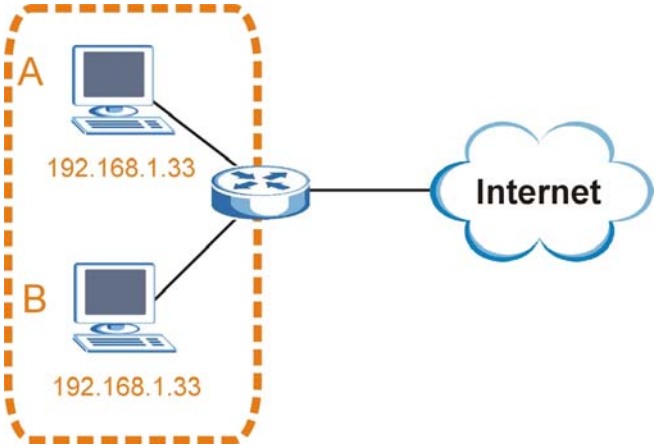
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

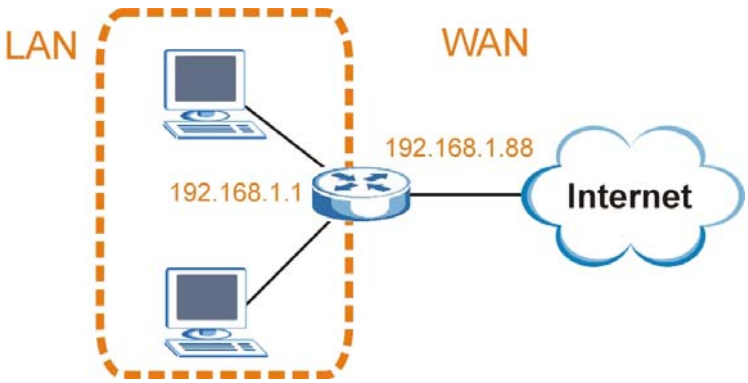
Figure 76 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

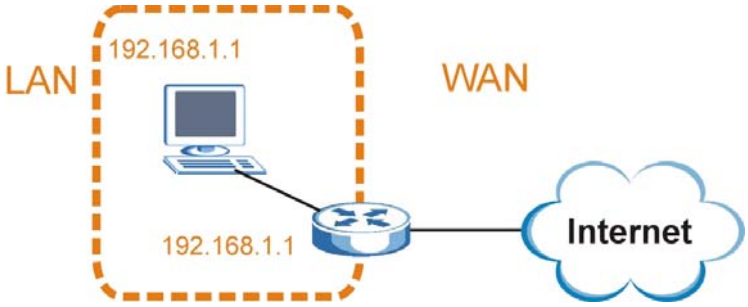
Figure 77 Conflicting Computer IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 78 Conflicting Computer and Router IP Addresses Example



B

Setting Up Your Computer's IP Address

Note: Your specific LTE Device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

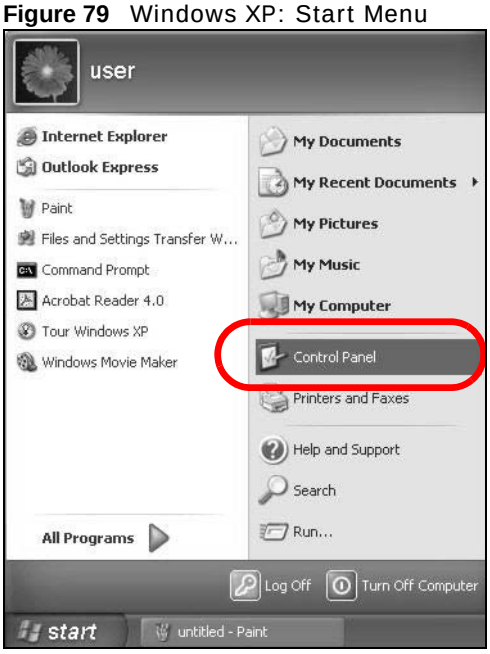
- Windows XP/NT/2000 on page 137
- Windows Vista on page 141
- Windows 7 on page 145
- Mac OS X: 10.3 and 10.4 on page 149
- Mac OS X: 10.5 on page 152
- Linux: Ubuntu 8 (GNOME) on page 156
- Linux: openSUSE 10.3 (KDE) on page 160

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

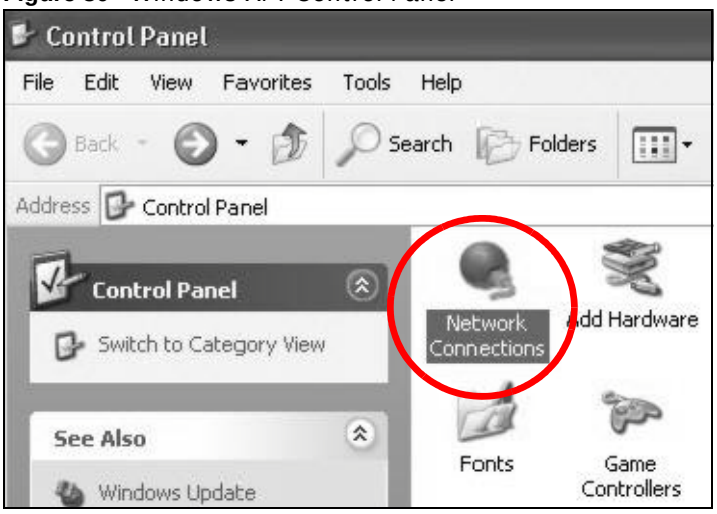
1 Click **Start** > **Control Panel**.

Figure 79 Windows XP: Start Menu



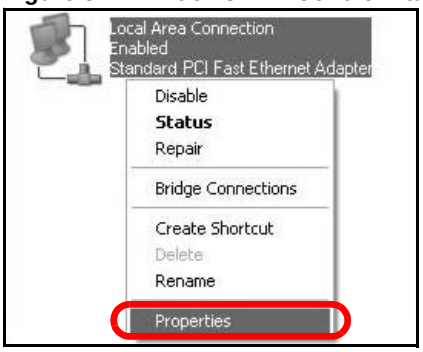
2 In the **Control Panel**, click the **Network Connections** icon.

Figure 80 Windows XP: Control Panel



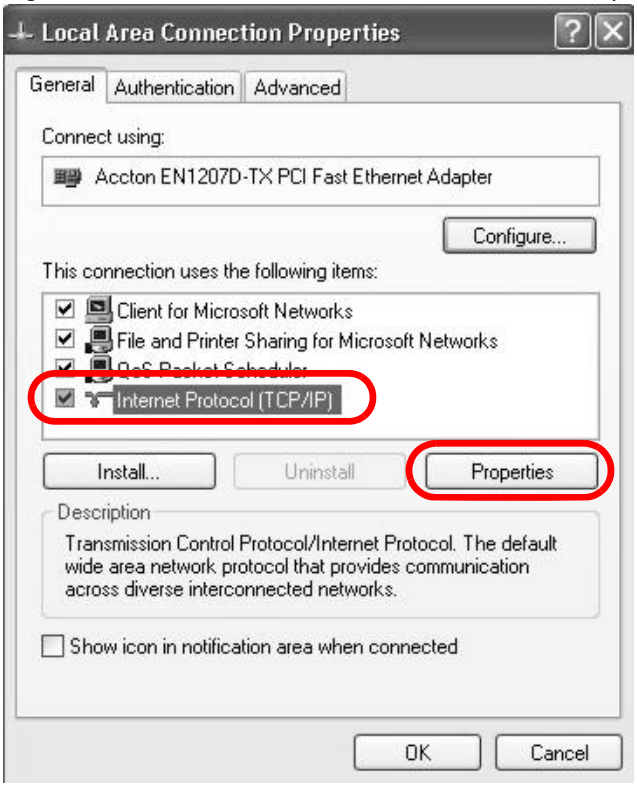
3 Right-click **Local Area Connection** and then select **Properties**.

Figure 81 Windows XP: Control Panel > Network Connections > Properties



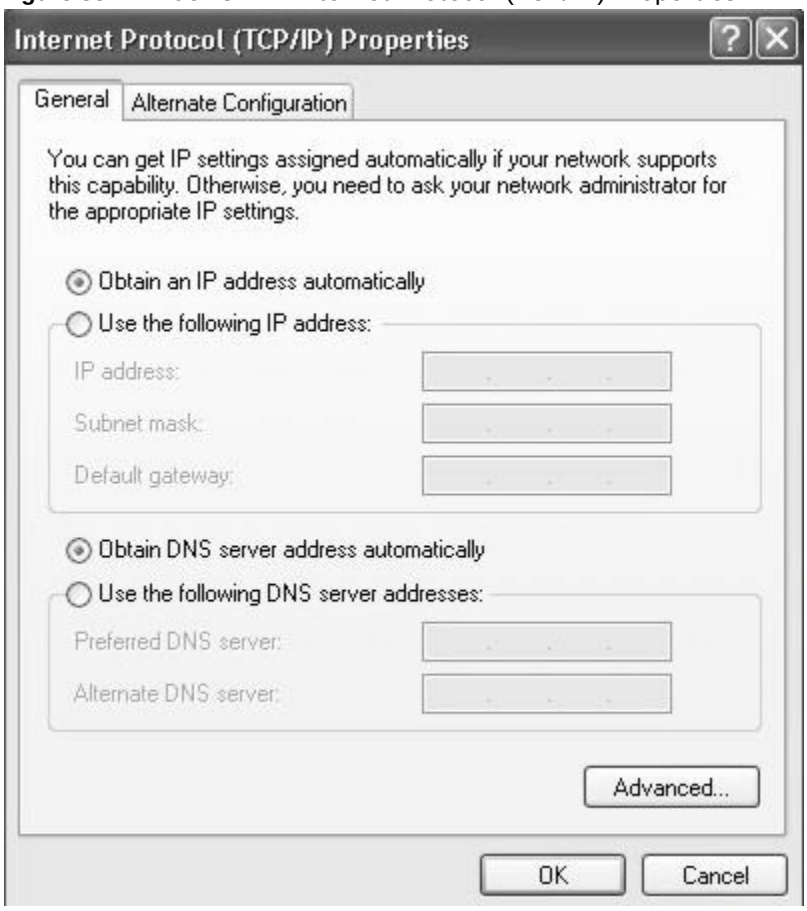
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 82 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 83 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

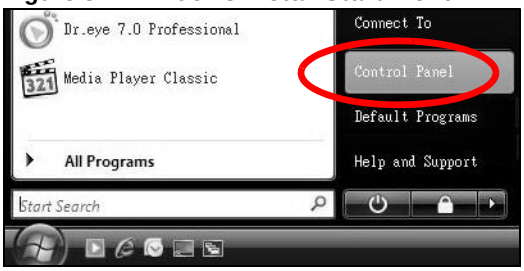
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

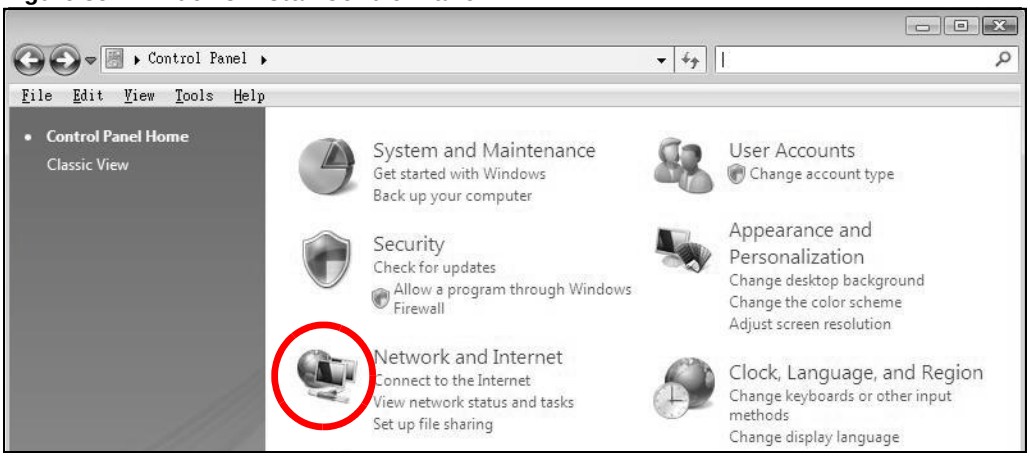
1 Click **Start** > **Control Panel**.

Figure 84 Windows Vista: Start Menu



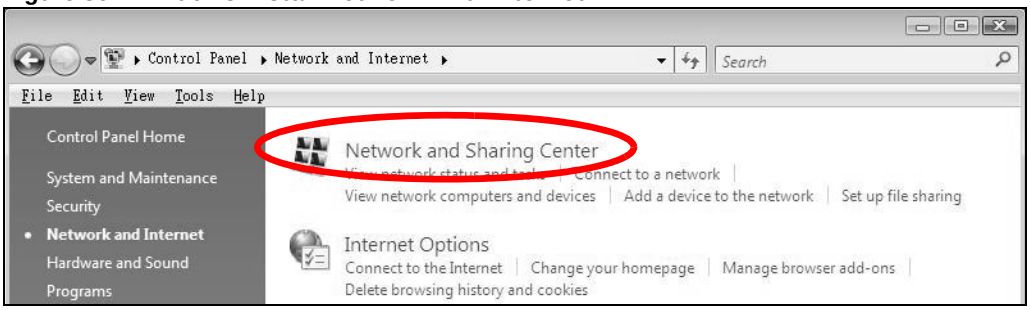
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 85 Windows Vista: Control Panel



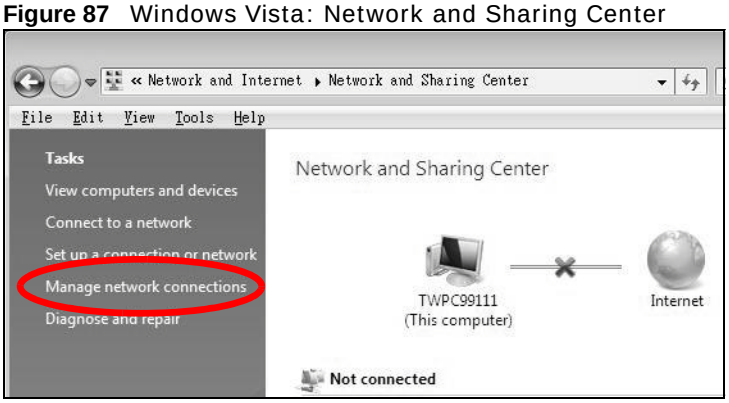
3 Click the **Network and Sharing Center** icon.

Figure 86 Windows Vista: Network And Internet



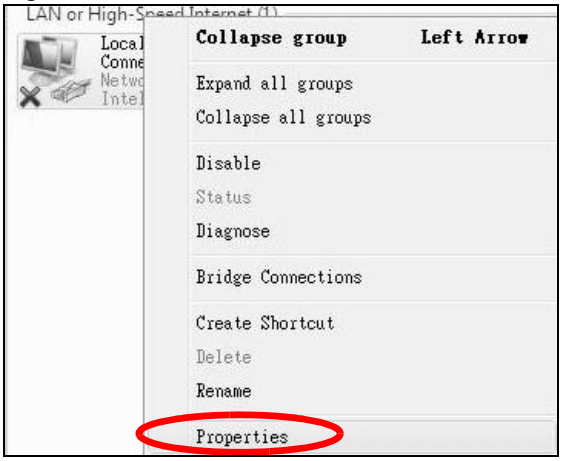
4 Click **Manage network connections**.

Figure 87 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then select **Properties**.

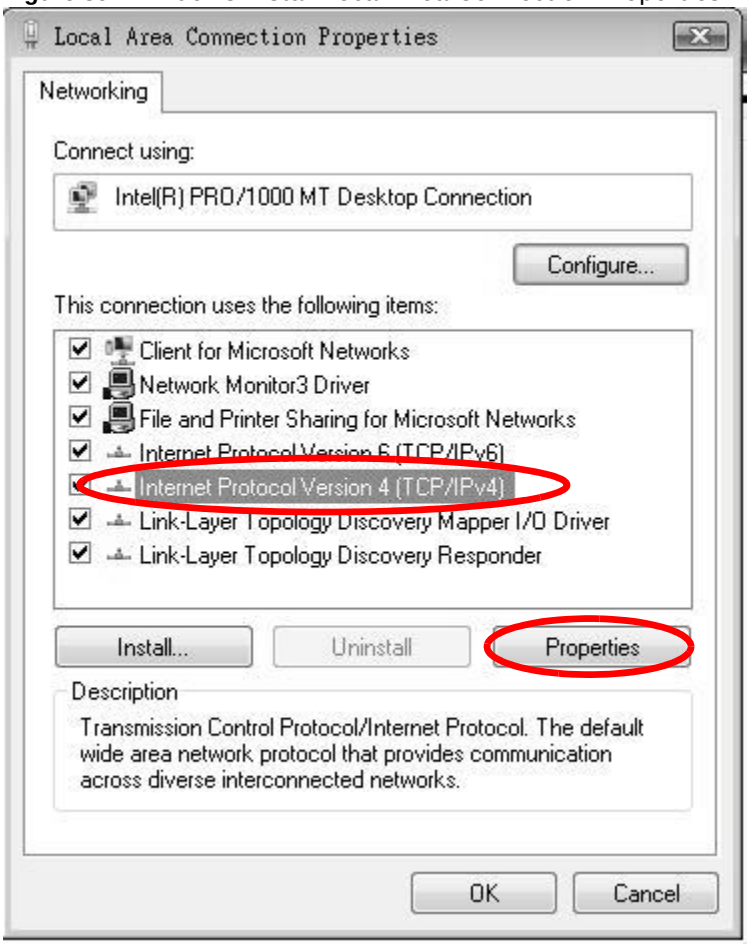
Figure 88 Windows Vista: Network and Sharing Center



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

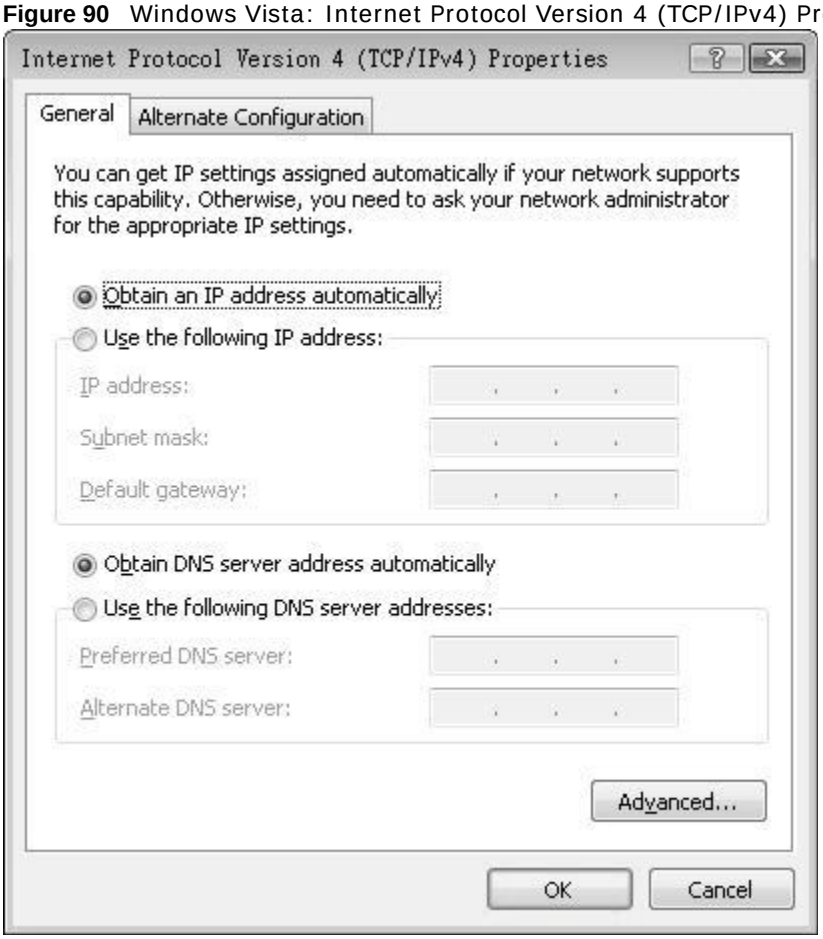
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 89 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 90 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

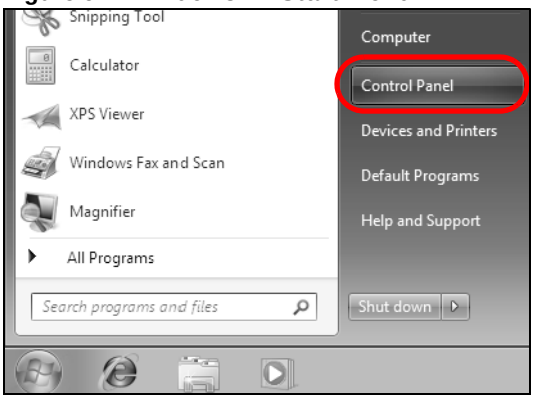
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

This section shows screens from Windows 7 Enterprise.

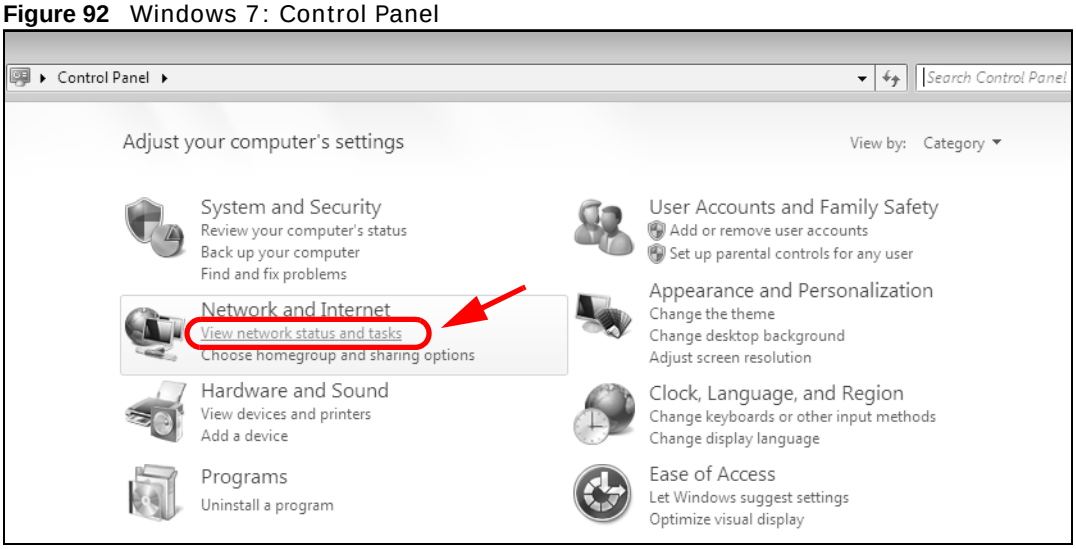
1 Click **Start** > **Control Panel**.

Figure 91 Windows 7: Start Menu



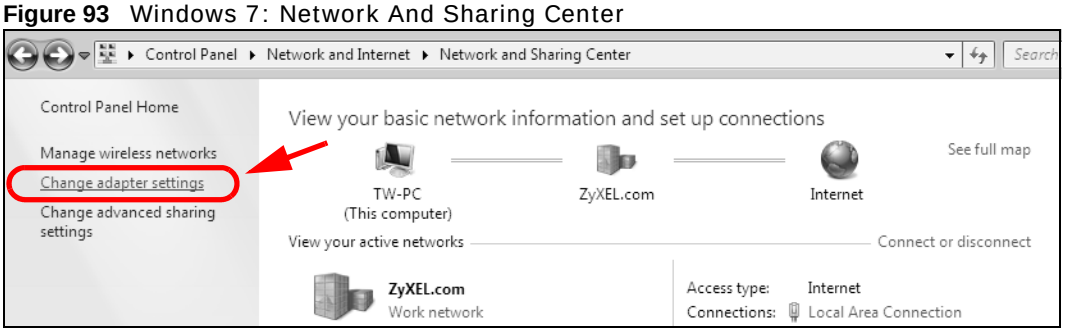
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 92 Windows 7: Control Panel



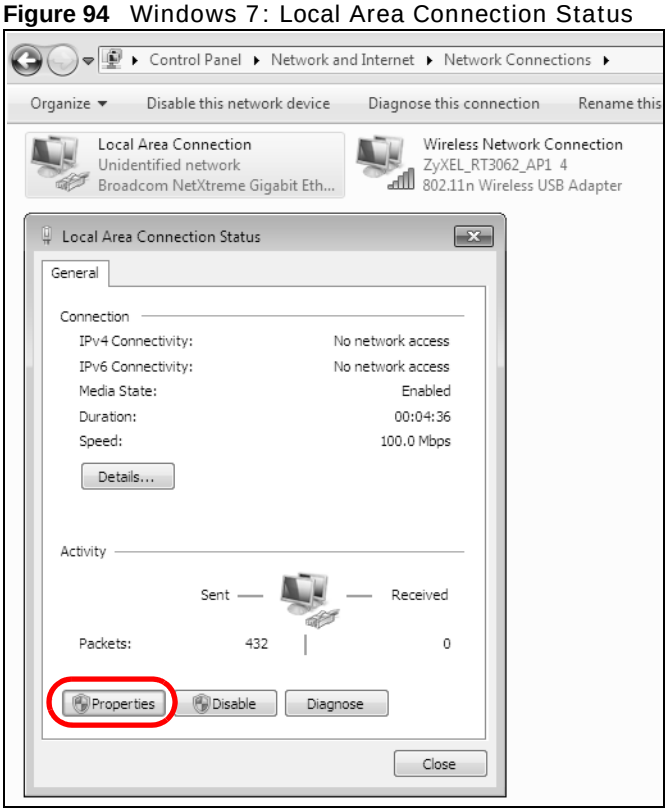
3 Click **Change adapter settings**.

Figure 93 Windows 7: Network And Sharing Center



4 Double click **Local Area Connection** and then select **Properties**.

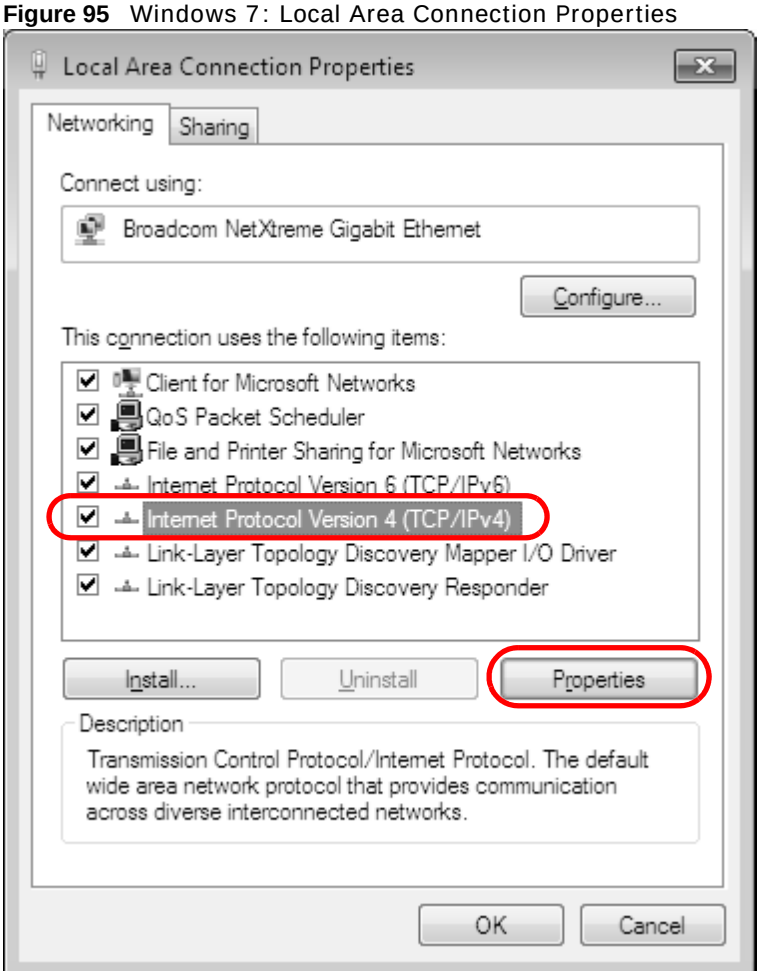
Figure 94 Windows 7: Local Area Connection Status



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

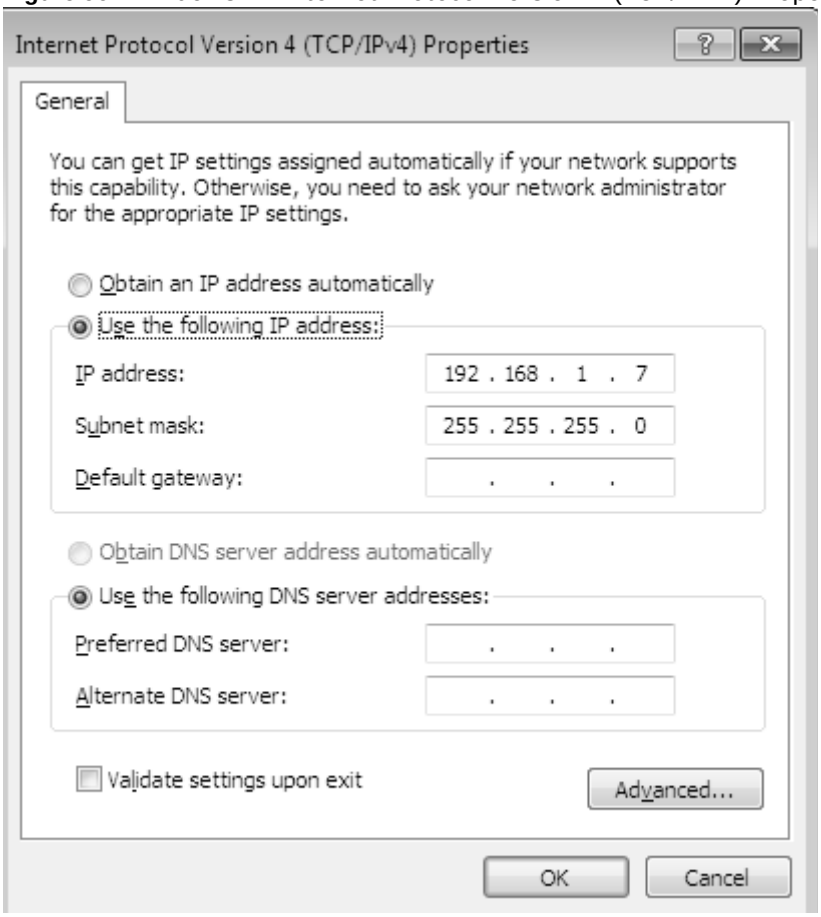
5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 95 Windows 7: Local Area Connection Properties



6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 96 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 7
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

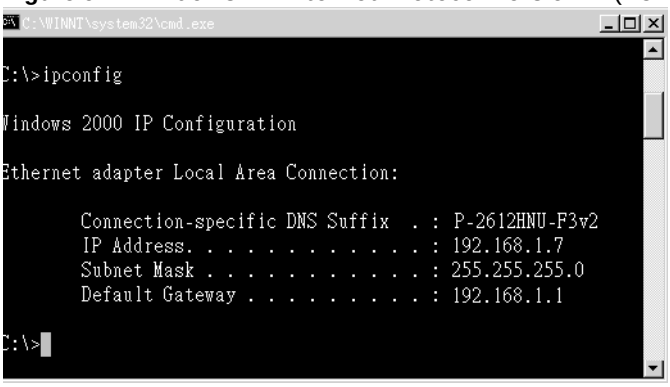
Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

3 The IP settings are displayed as follows.

Figure 97 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties


C:\WINNT\system32\cmd.exe
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : P-2612HNU-F3v2
IP Address. . . . . : 192.168.1.7
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\>

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

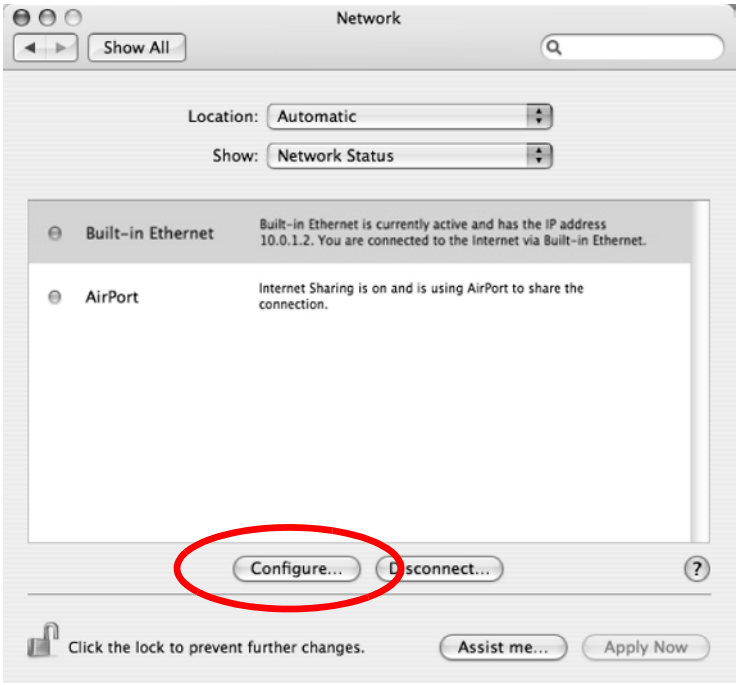
Figure 98 Mac OS X 10.4: Apple Menu

2 In the **System Preferences** window, click the **Network** icon.

Figure 99 Mac OS X 10.4: System Preferences

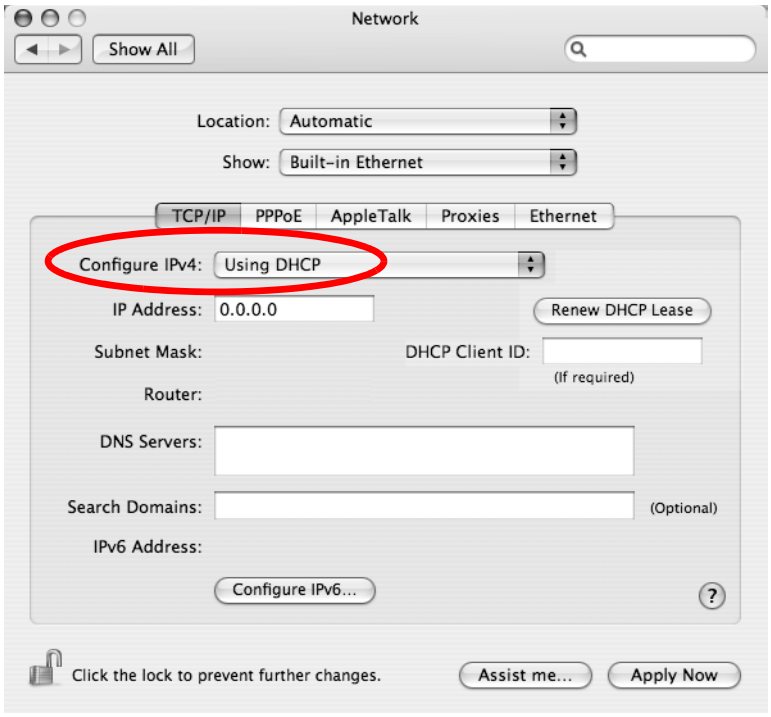
3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 100 Mac OS X 10.4: Network Preferences


Network
Show All
Location: Automatic
Show: Network Status
Built-in Ethernet
Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.
AirPort
Internet Sharing is on and is using AirPort to share the connection.
Configure...
Disconnect...
Click the lock to prevent further changes.
Assist me...
Apply Now

4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 101 Mac OS X 10.4: Network Preferences > TCP/IP Tab.

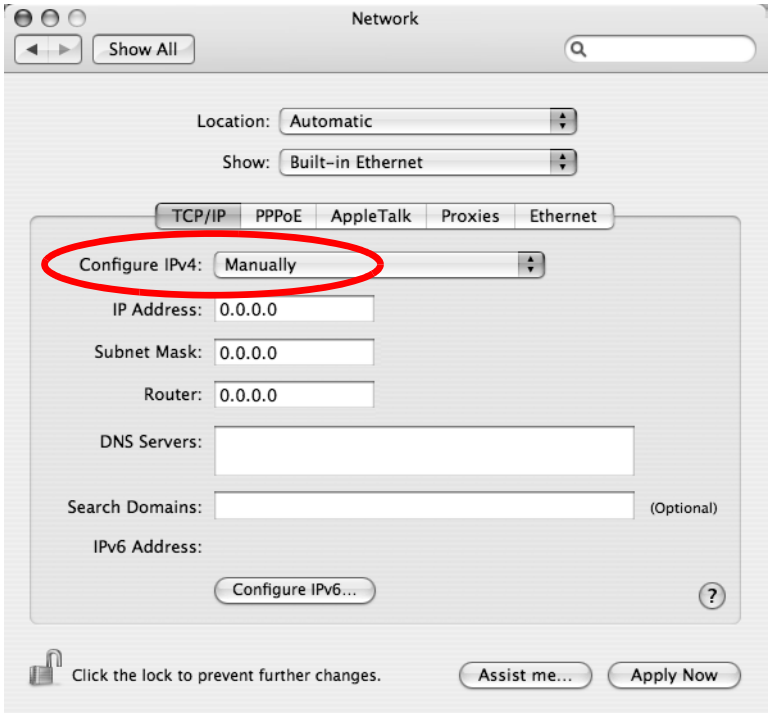


5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.

- In the **Router** field, type the IP address of your device.

Figure 102 Mac OS X 10.4: Network Preferences > Ethernet

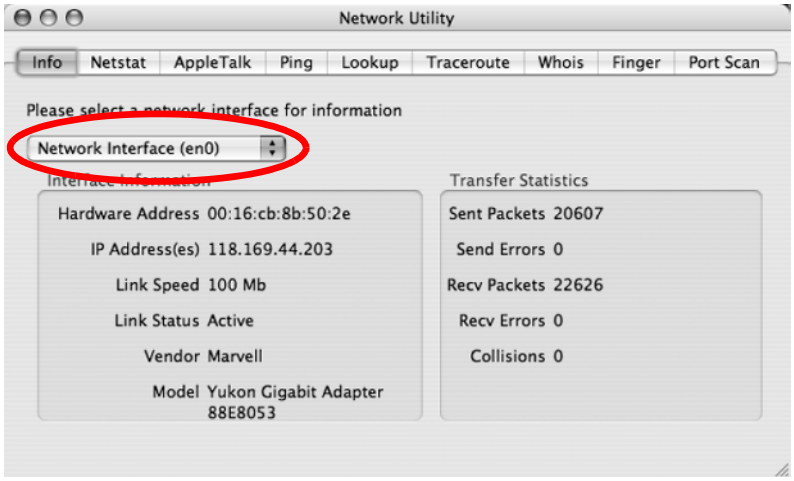


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 103 Mac OS X 10.4: Network Utility

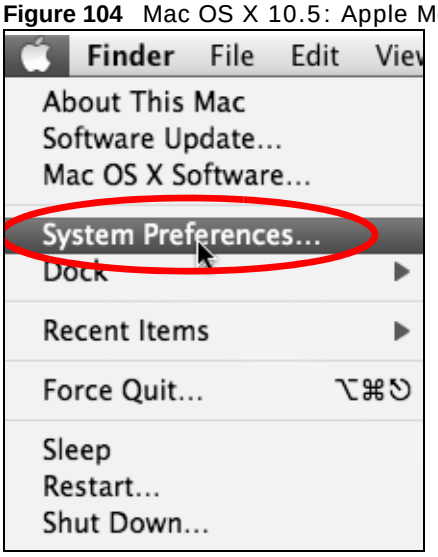


Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

1 Click **Apple** > **System Preferences**.

Figure 104 Mac OS X 10.5: Apple Menu

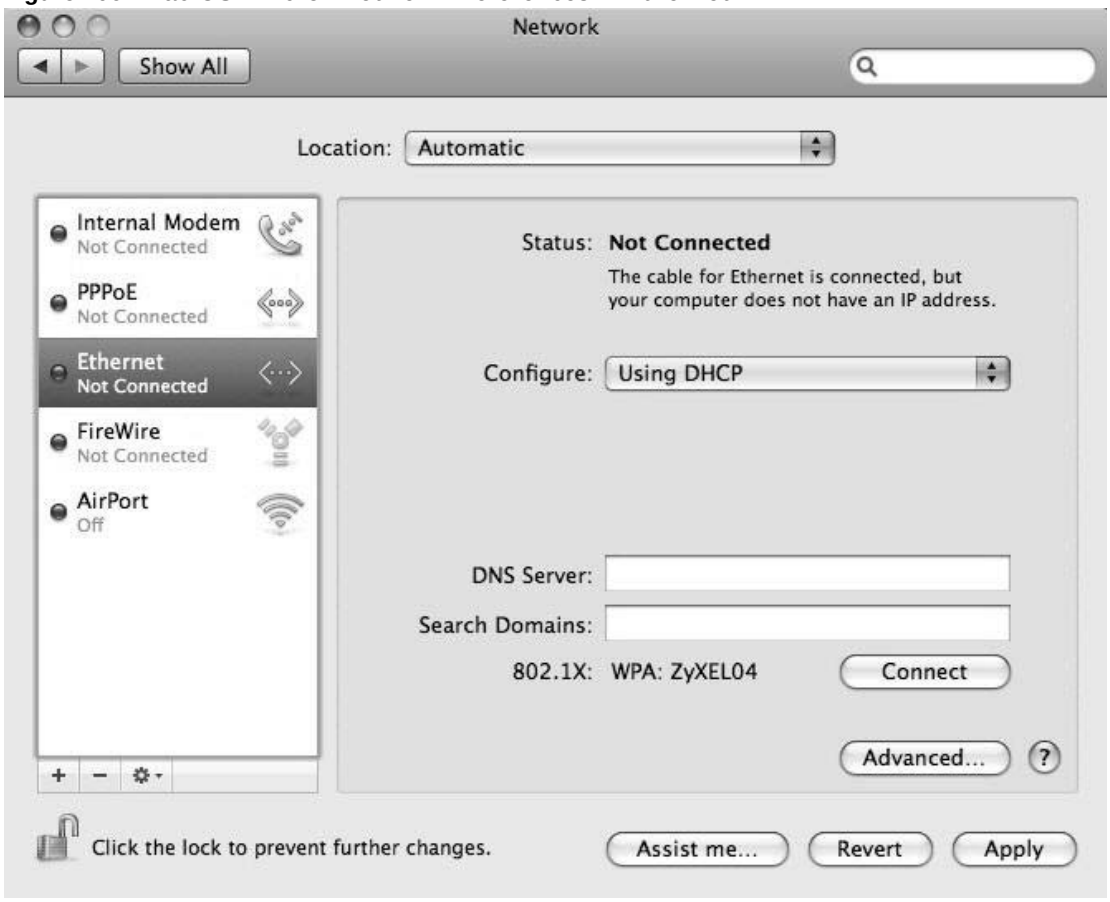


2 In **System Preferences**, click the **Network** icon.

Figure 105 Mac OS X 10.5: Systems Preferences

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 106 Mac OS X 10.5: Network Preferences > Ethernet



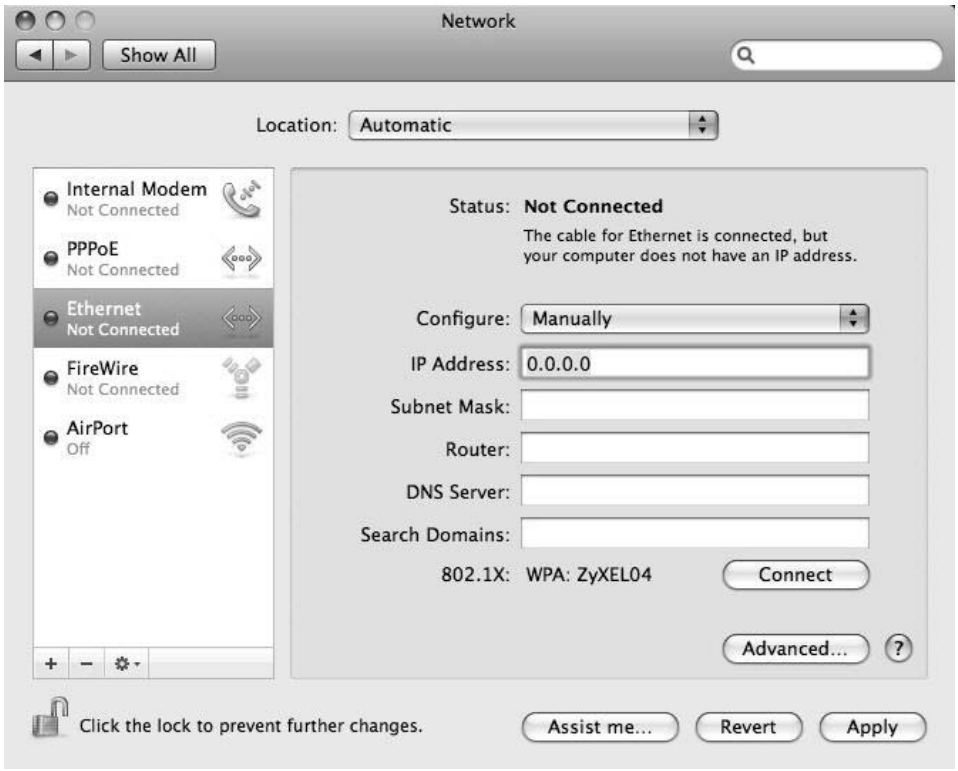
4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your LTE Device.

Figure 107 Mac OS X 10.5: Network Preferences > Ethernet

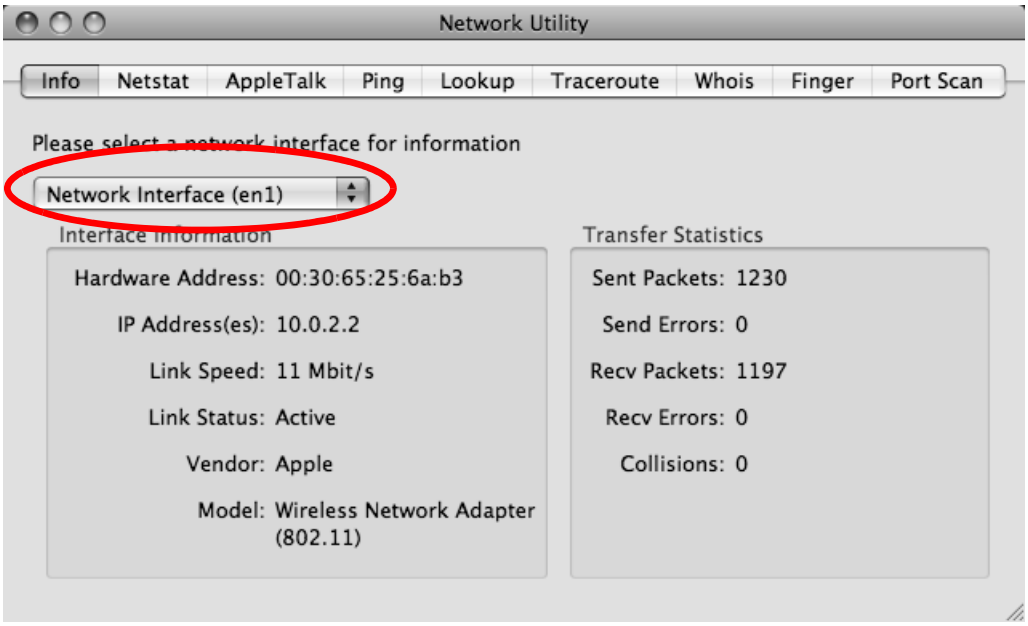


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 108 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

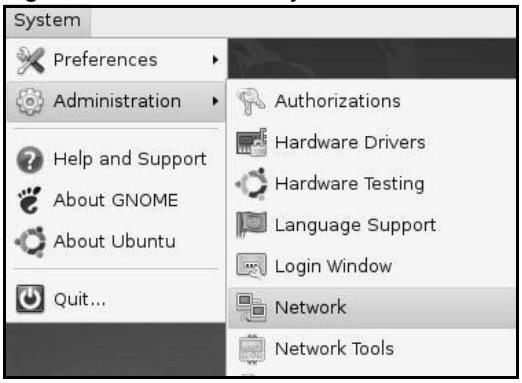
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

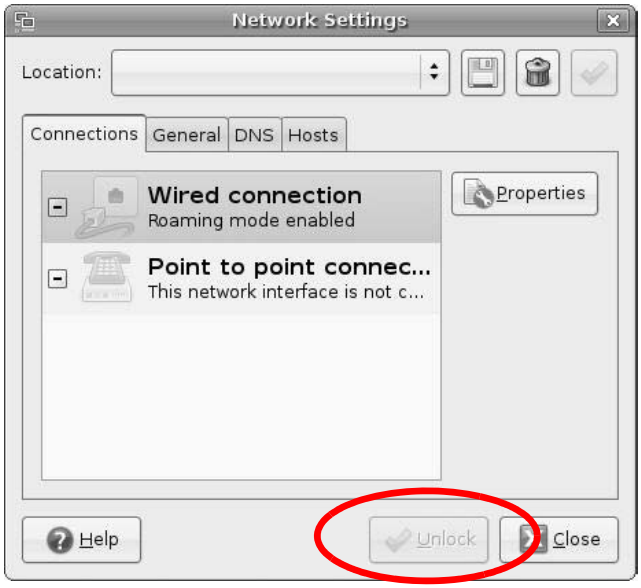
1 Click **System > Administration > Network**.

Figure 109 Ubuntu 8: System > Administration Menu



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 110 Ubuntu 8: Network Settings > Connections



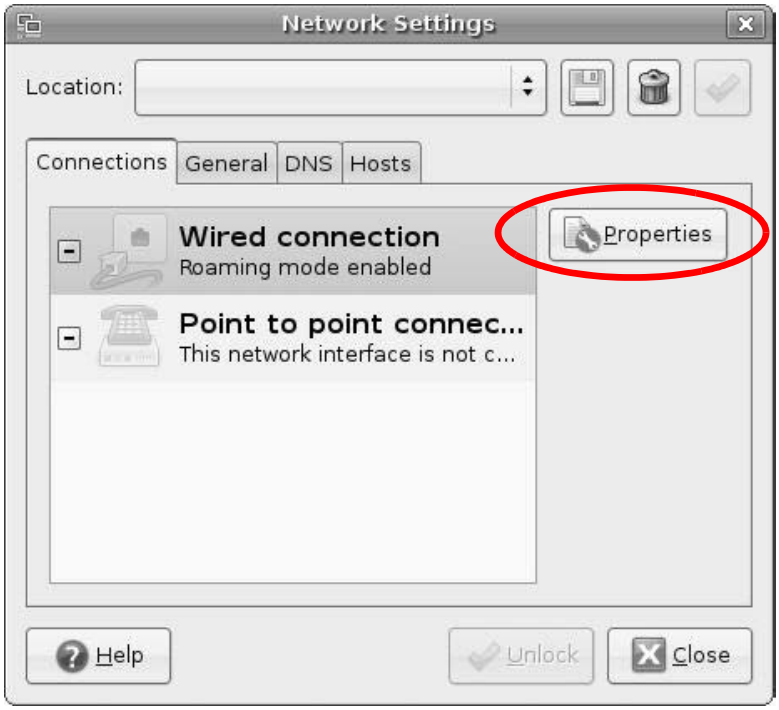
3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 111 Ubuntu 8: Administrator Account Authentication

Authenticate
System policy prevents modifying the configuration
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.
C.J.,,,, (chris)
Password for chris:
Details
Cancel
Authenticate

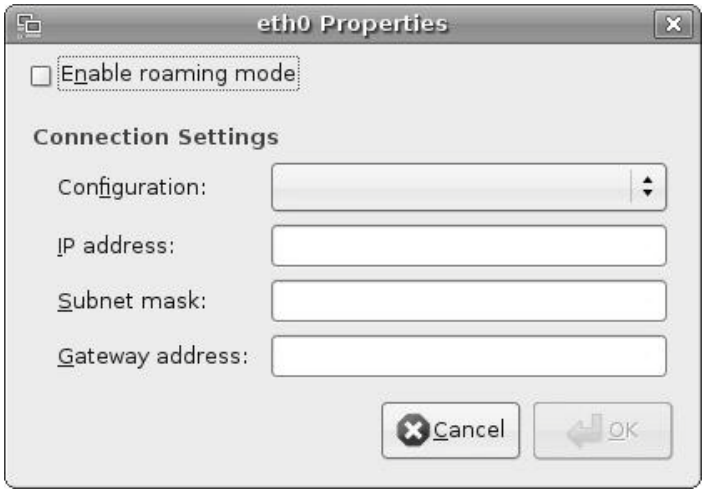
4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 112 Ubuntu 8: Network Settings > Connections



5 The **Properties** dialog box opens.

Figure 113 Ubuntu 8: Network Settings > Properties

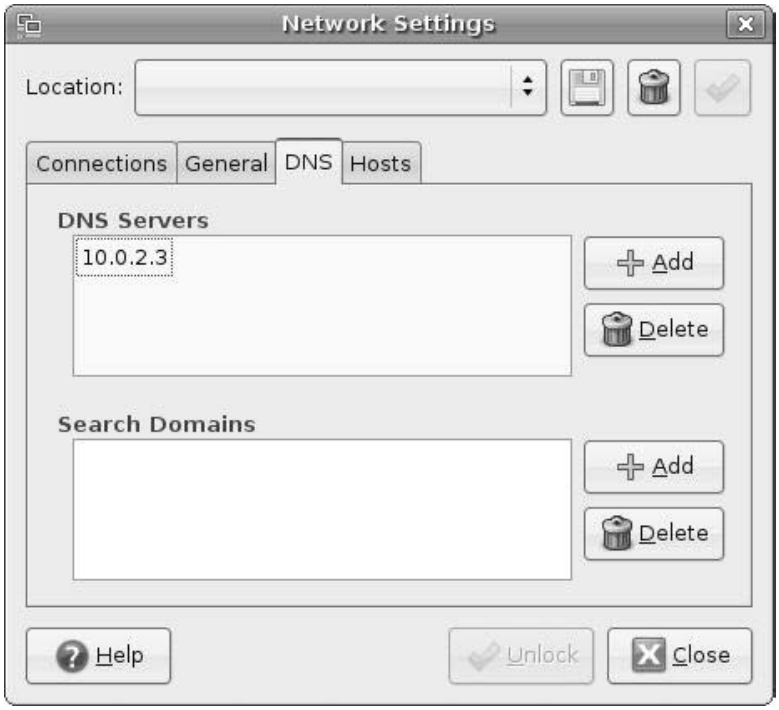


- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 114 Ubuntu 8: Network Settings > DNS

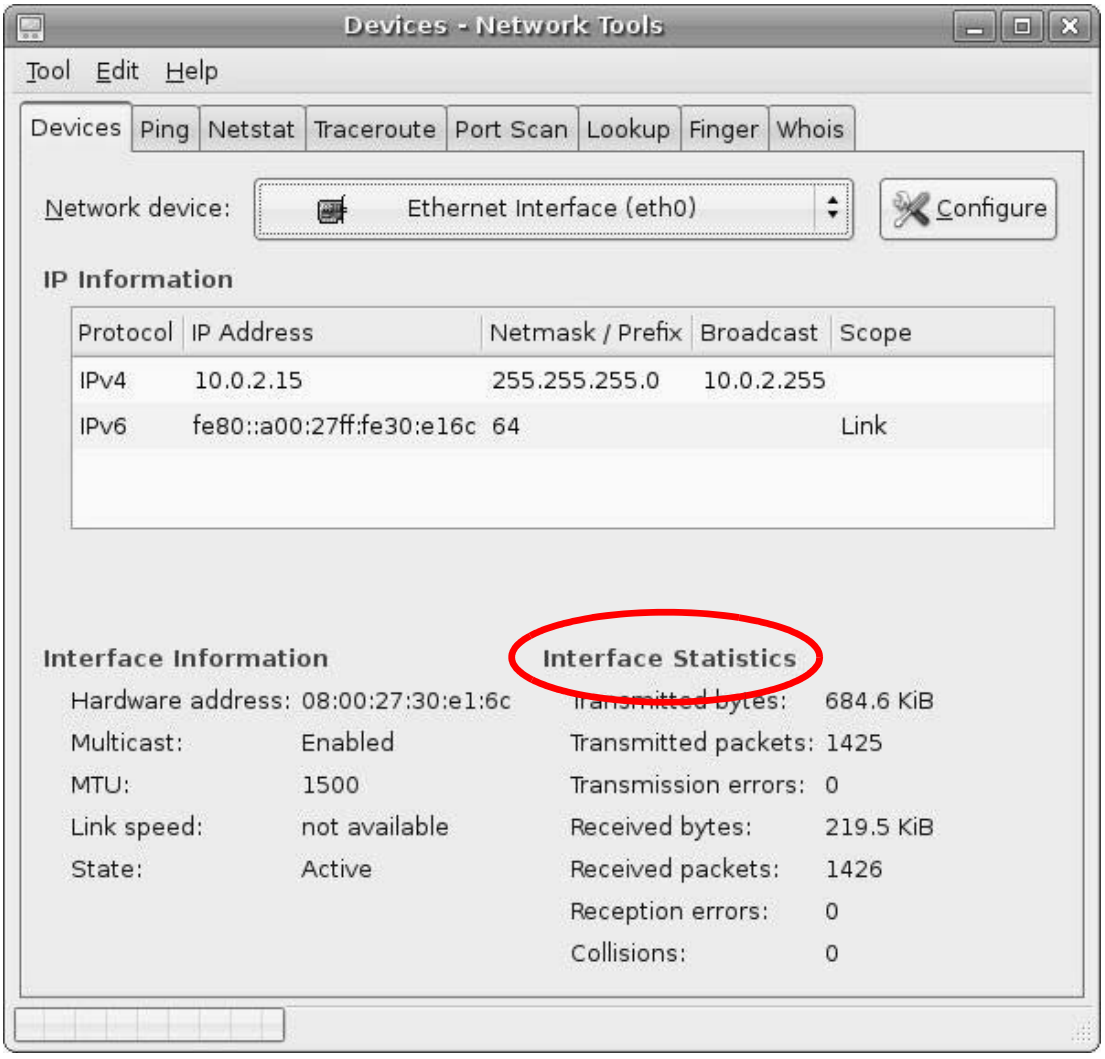


8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 115 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

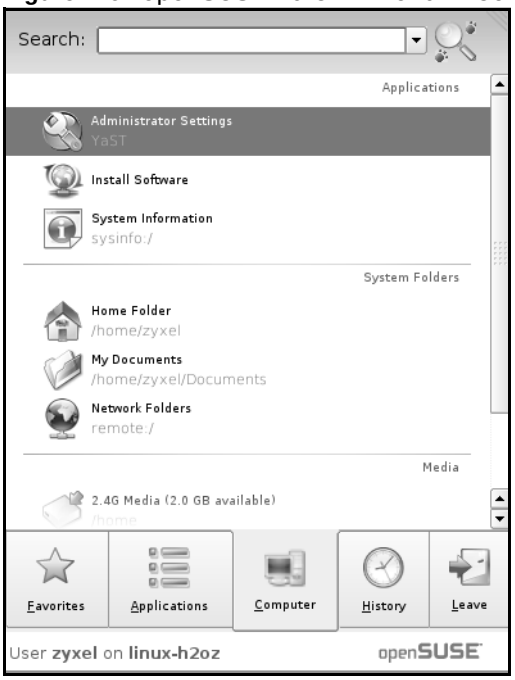
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

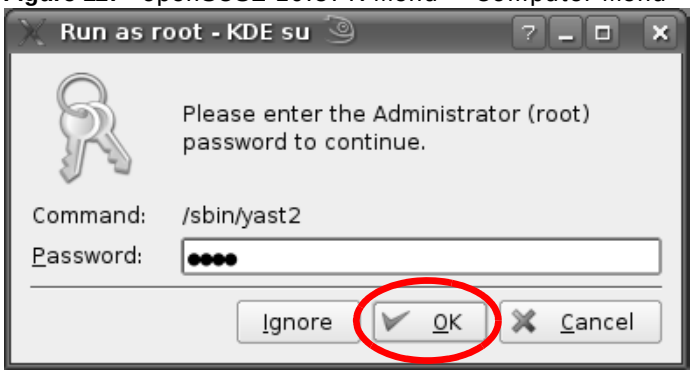
1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 116 openSUSE 10.3: K Menu > Computer Menu



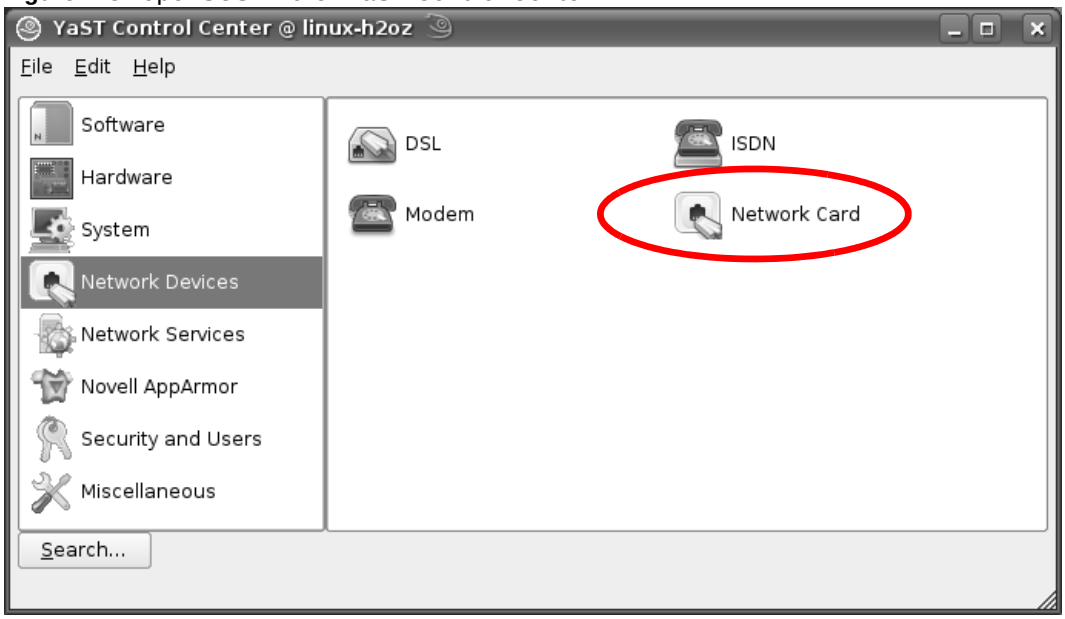
2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 117 openSUSE 10.3: K Menu > Computer Menu



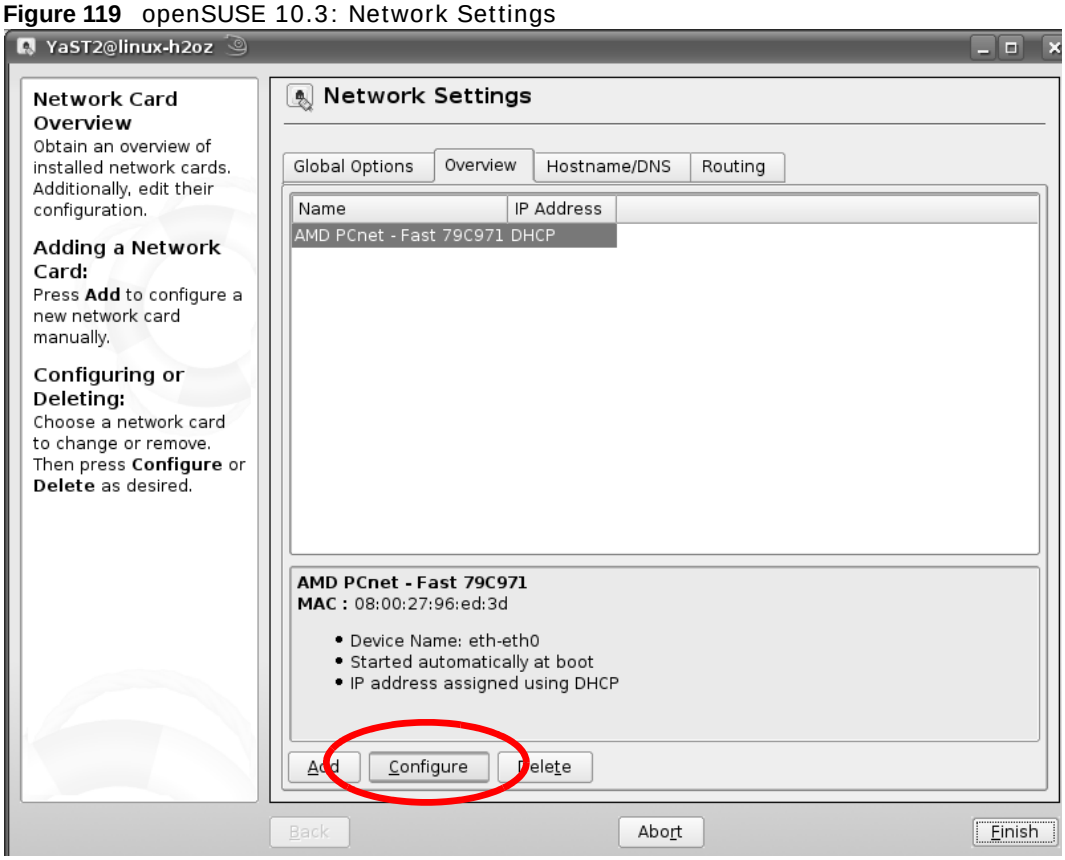
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 118 openSUSE 10.3: YaST Control Center



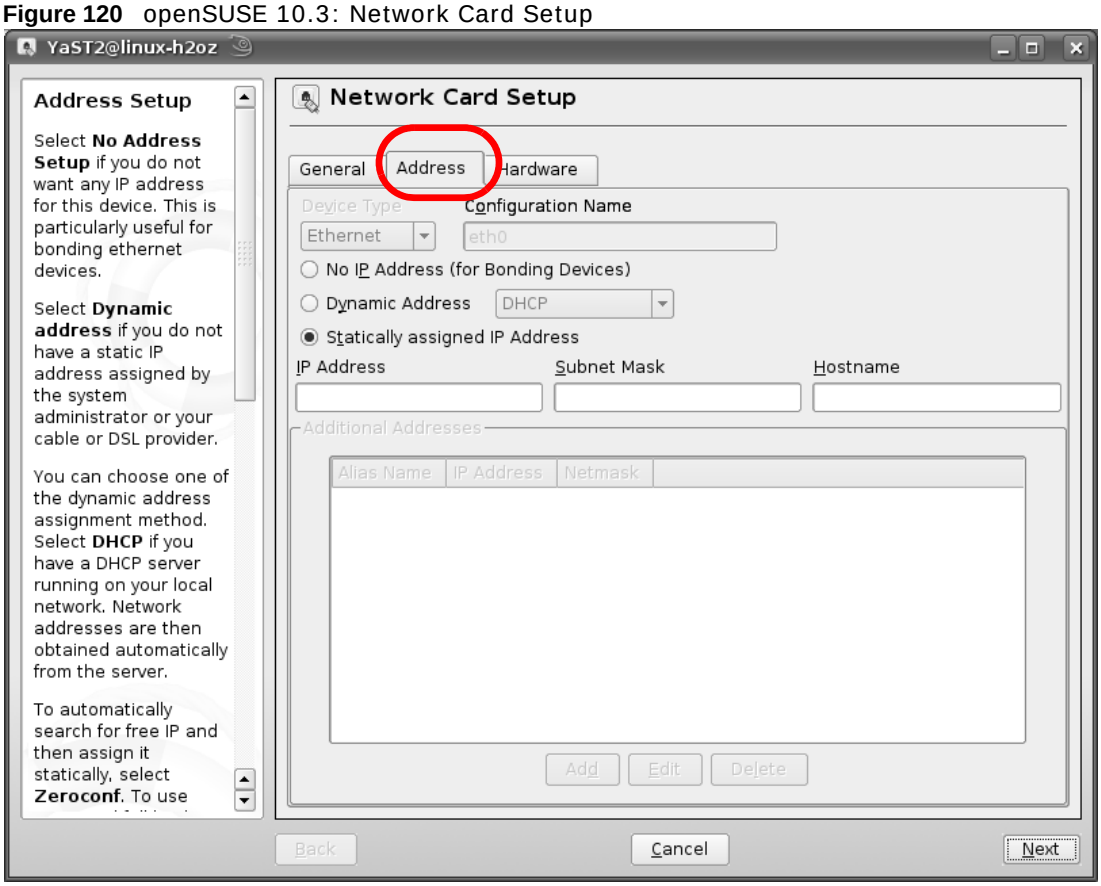
4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 119 openSUSE 10.3: Network Settings



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 120 openSUSE 10.3: Network Card Setup


YaST2@linux-h2oz
Address Setup
Select No Address Setup if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.
Select Dynamic address if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.
You can choose one of the dynamic address assignment method. Select DHCP if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.
To automatically search for free IP and then assign it statically, select Zeroconf. To use
Network Card Setup
General
Address
Hardware
Device Type
Configuration Name
Ethernet
eth0
No IP Address (for Bonding Devices)
Dynamic Address
DHCP
Statically assigned IP Address
IP Address
Subnet Mask
Hostname
Additional Addresses
Alias Name
IP Address
Netmask
Add
Edit
Delete
Back
Cancel
Next

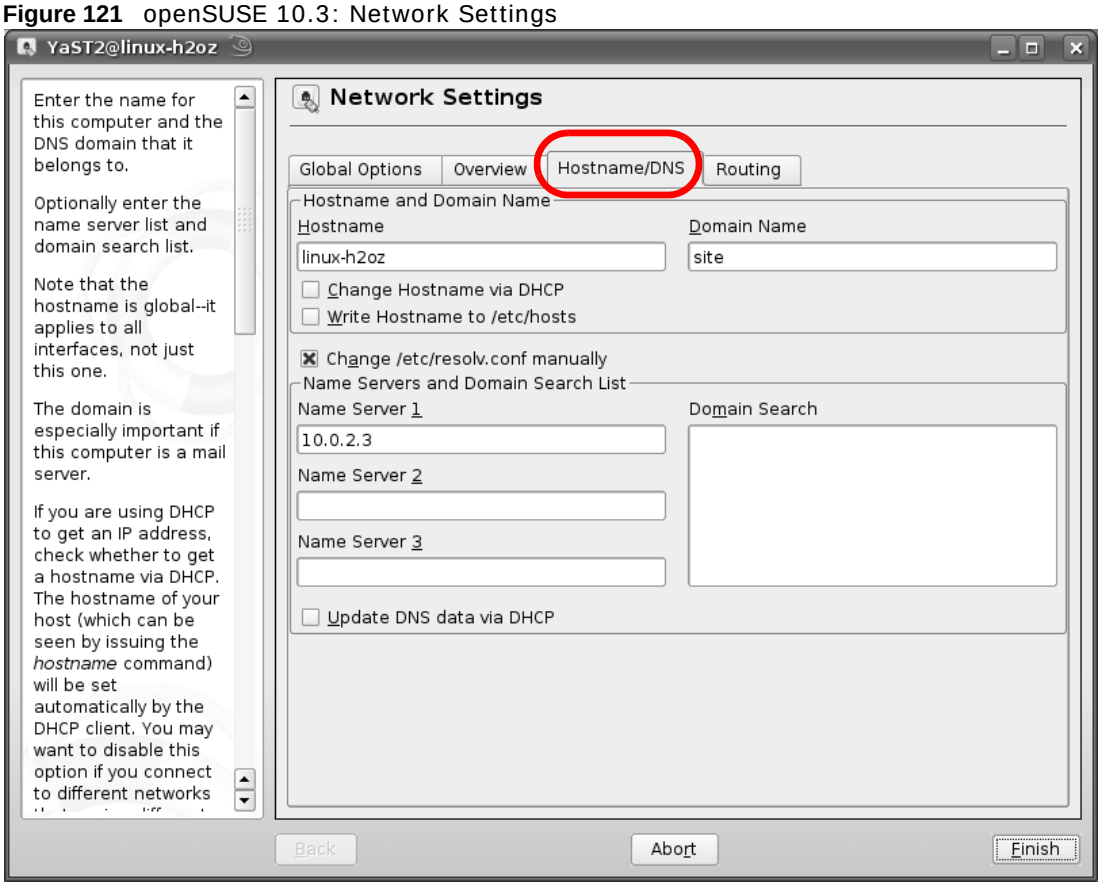
6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 121 openSUSE 10.3: Network Settings

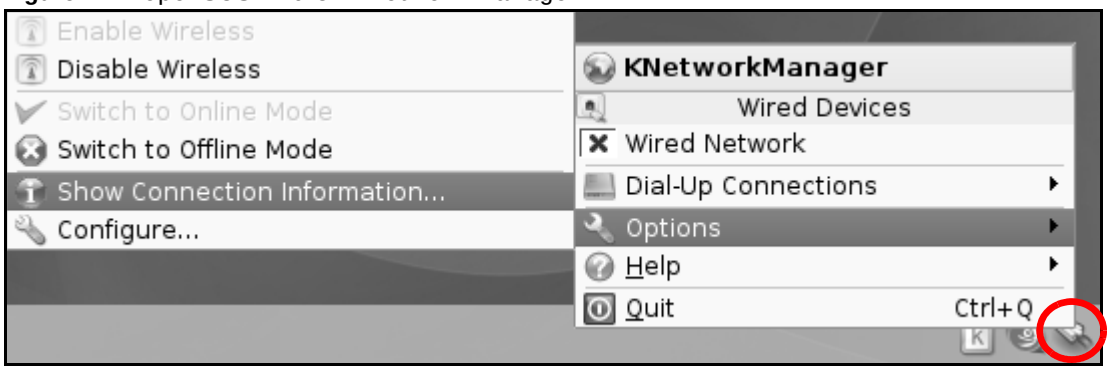

YaST2@linux-h2oz
Enter the name for this computer and the DNS domain that it belongs to.
Optionally enter the name server list and domain search list.
Note that the hostname is global--it applies to all interfaces, not just this one.
The domain is especially important if this computer is a mail server.
If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the hostname command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks
Network Settings
Global Options
Overview
Hostname/DNS
Routing
Hostname and Domain Name
Hostname
linux-h2oz
Domain Name
site
Change Hostname via DHCP
Write Hostname to /etc/hosts
Change /etc/resolv.conf manually
Name Servers and Domain Search List
Name Server 1
10.0.2.3
Domain Search
Name Server 2
Name Server 3
Update DNS data via DHCP
Back
Abort
Finish

9 Click **Finish** to save your settings and close the window.

Verifying Settings

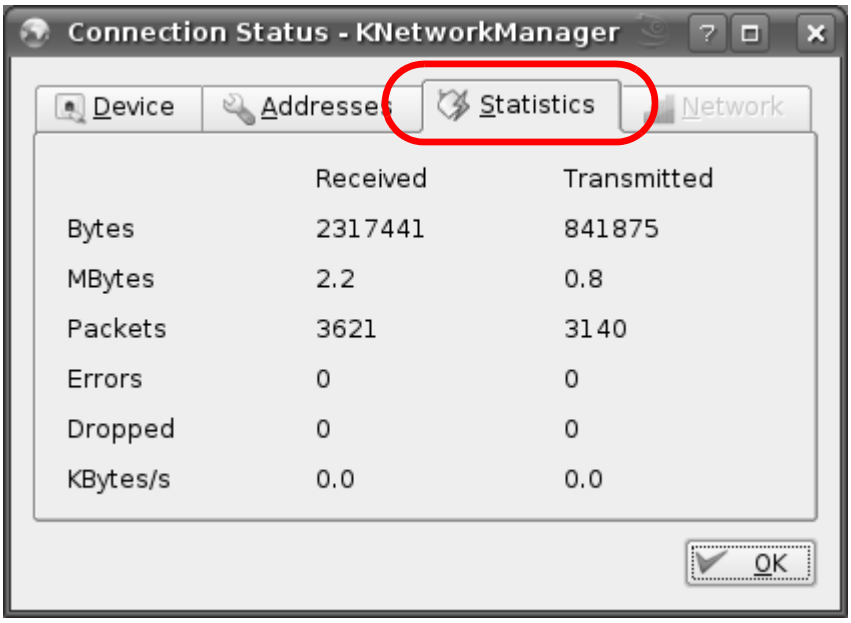
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 122 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 123 openSUSE: Connection Status - KNetwork Manager



C

Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

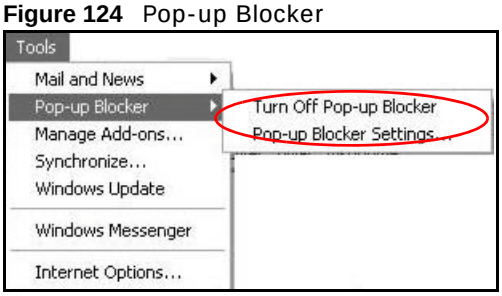
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 124 Pop-up Blocker

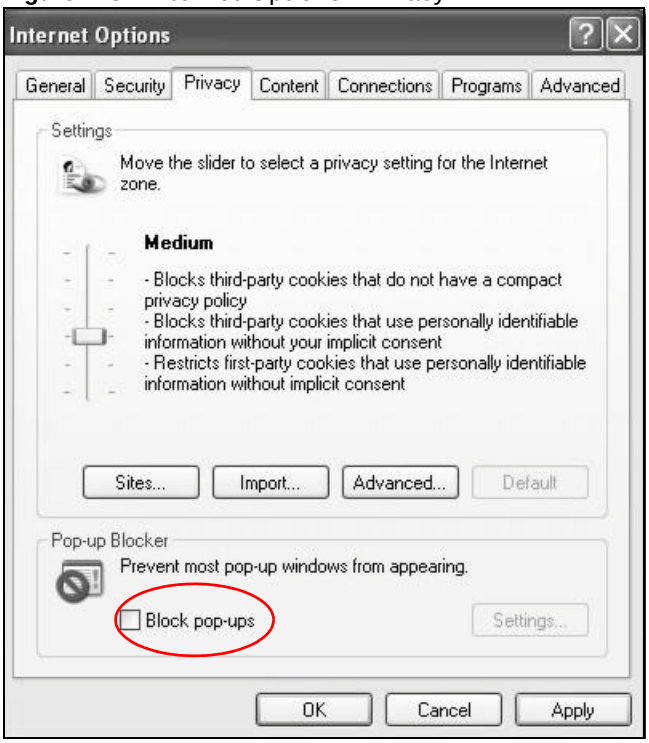


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 125 Internet Options: Privacy



3 Click **Apply** to save this setting.

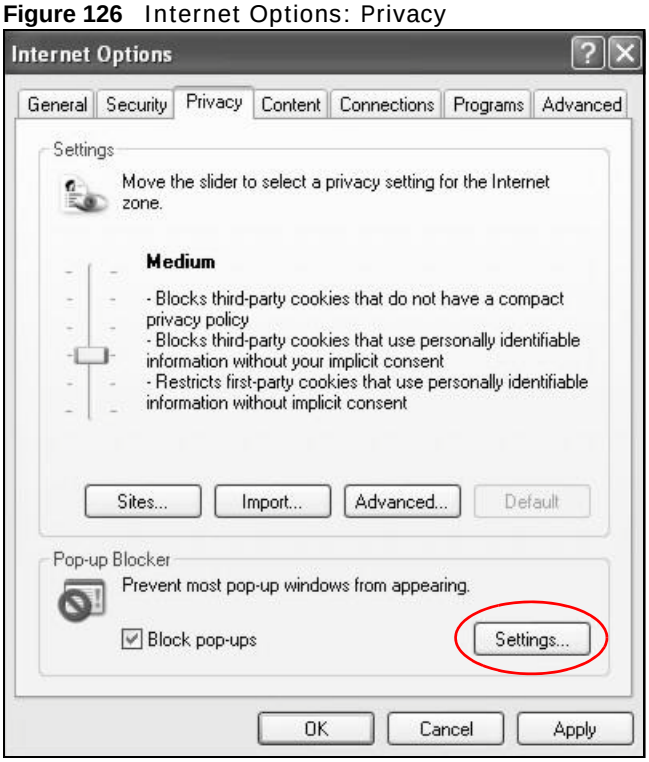
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

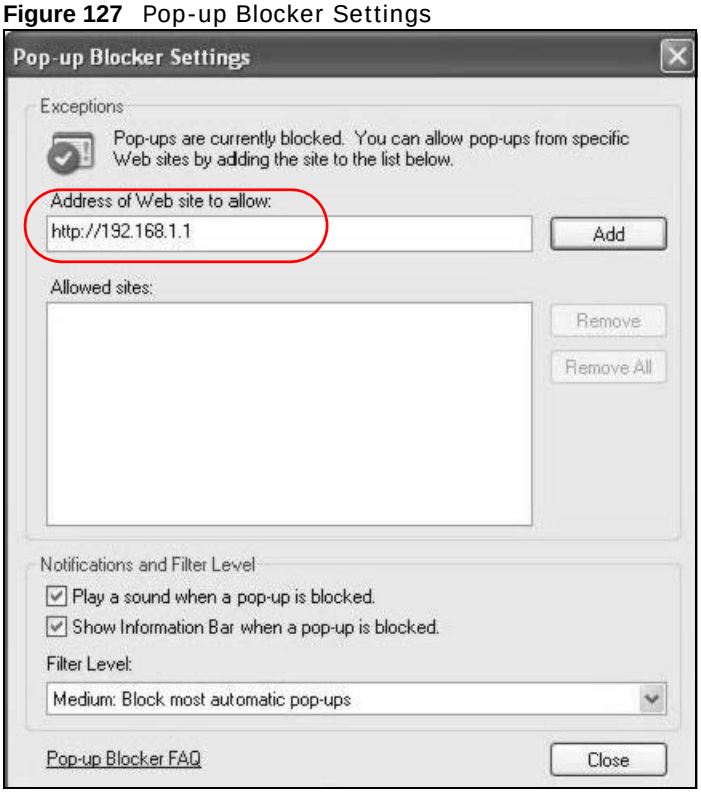
Figure 126 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 127 Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

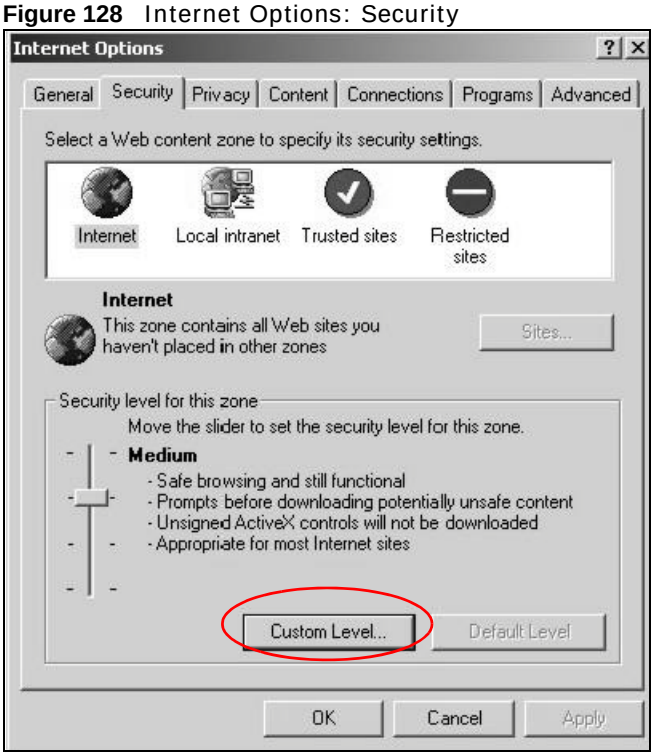
6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 128 Internet Options: Security



2 Click the **Custom Level...** button.

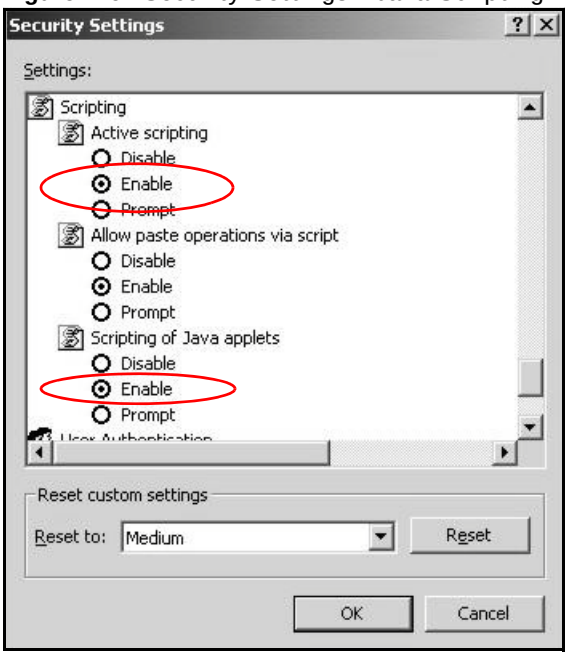
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 129 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

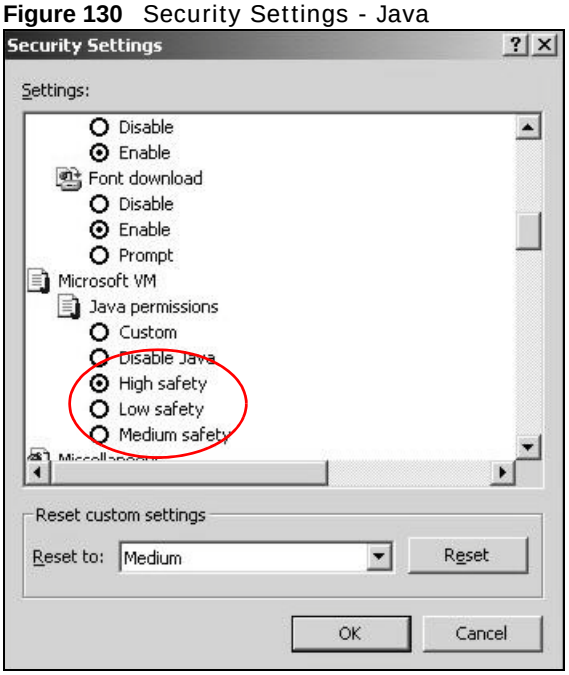
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 130 Security Settings - Java



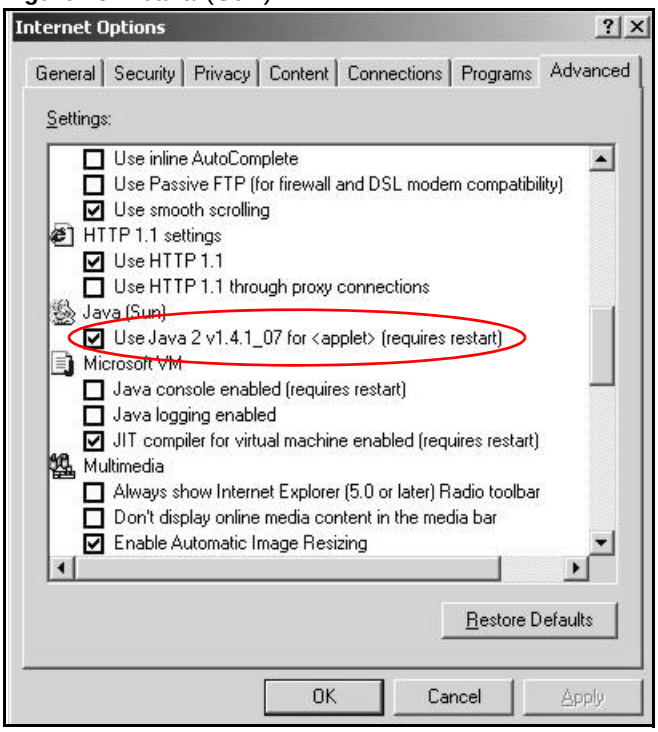
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 131 Java (Sun)

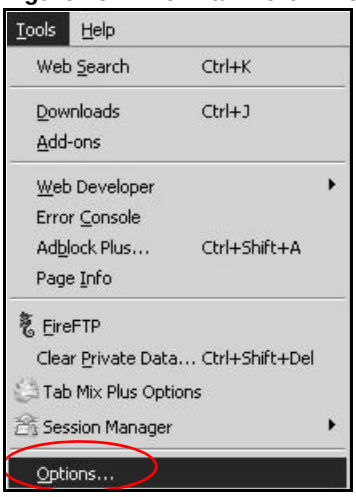


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

You can enable Java, JavaScript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 132 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 133 Mozilla Firefox Content Security

D

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 68 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.example.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.

Table 68 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.

Table 68 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

E

Legal Information

Copyright

Copyright © 2012 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the LTE Device is subject to the terms and conditions of any related service providers.

Do not use the LTE Device for illegal purposes. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws, and will bear the consequences of any infringements thereof. ZyXEL bears NO responsibility or liability for your use of the download service feature.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device complies with part 15 of the FCC Rules.
- Operation is subject to the condition that this device does not cause harmful interference.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause

harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the indoor device (IDU) outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index

A

administrator password 17
AH 92
algorithms 92
alternative subnet mask notation 130
applications
  Internet access 13
automatic logout 18

B

backup
  configuration 117
bandwidth management 49
blinking LEDs 15
Broadband 31

C

certification
  notices 182
  viewing 182
client list 42
configuration
  backup 117
  reset 119
  restoring 118
copyright 181
CoS 57

D

default LAN IP address 17
Denials of Service, see DoS
DH 98
DHCP 28, 40, 67
diagnostic 121
Differentiated Services, see DiffServ
Diffie-Hellman key groups 98
DiffServ (Differentiated Services)
  marking rule 58
DNS 40
DNS server address assignment 35
documentation
  related 2
domain name system, see DNS
Domain Name System. See DNS.
DoS 70
DS (Differentiated Services) 57
DS field 57
DSCP 57
dynamic DNS 67
Dynamic Host Configuration Protocol, see DHCP
DYNDNS wildcard 67

E

Encapsulation 35
encapsulation 93
ESP 92

F

FCC interference statement 181
firewalls 69
  configuration 72
  DoS 70
  security 76
firmware 115
FTP 60

G

Guide
  Quick Start 2

H

host 105
host name 27

I

IANA 134
ID type and content 96
IKE phases 94
inside header 93
Internet access 13
Internet Assigned Numbers Authority, see IANA
Internet Key Exchange 94
IP address 28
  default 17
  WAN 31
IP Address Assignment 35
IP pool 41
IPSec
  algorithms 92
  architecture 92
  NAT 95
IPSec VPN 85

L

LAN 39
  client list 42
  MAC address 43
Local Area Network, see LAN
login
  passwords 17
logout 18
  automatic 18
logs 99, 113

M

MAC 27, 79
MAC address 43
MAC address filtering 79
MAC filter 79
managing the device
  good habits 14
  using FTP. See FTP.
Media access control 79
Media Access Control, see MAC Address
model name 27

N

NAT 60, 134
  definitions 64
  how it works 65
  IPSec 95
  traversal 96
  what it does 64
negotiation mode 94
Network Address Translation, see NAT
network map 21

O

other documentation 2
outside header 93

P

passwords 17
PHB 58
ports 15
pre-shared key 97
product registration 183

Q

QoS 49, 57
Quality of Service, see QoS
Quick Start Guide 2, 17

R

registration
  product 183
related documentation 2
reset 119
RESET button 15
restart 119
restoring configuration 118
RFC 1631 59
RFC 3164 99
router features 13

S

safety warnings 183
security, network 76
service access control 107
static route 45
status 25
status indicators 15
subnet 127
subnet mask 128
subnetting 130
syslog
  protocol 99
  severity levels 99
system
  firmware 115
  passwords 17
  status 25
System Info 27
system name 27, 110

T

The 31
transport mode 93
tunnel mode 93

U

Universal Plug and Play, see UPnP
upgrading firmware 115
UPnP 43
  security issues 40

V

version
  firmware
    version 27

W

WAN
  Wide Area Network, see WAN 31
warnings 183
Web Configurator 17
web configurator
  passwords 17